NICT NEWS
National Institute of Information and Communication Technology
No.5
2026
Vol.519

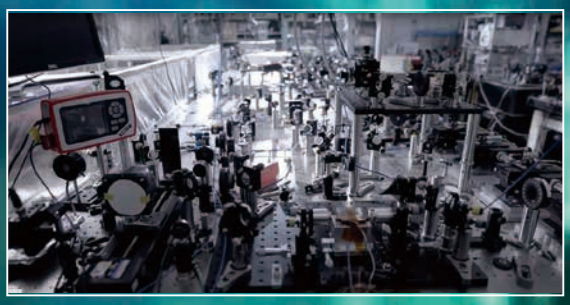
FEATURE

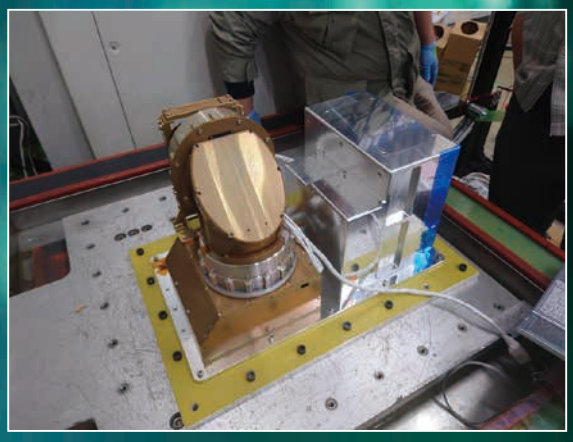
Harnessing the Quantum World: The Future of ICT

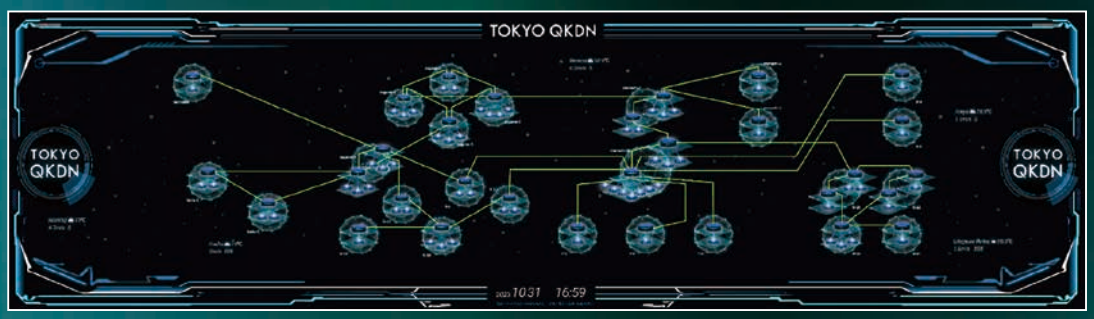
DIALOG

The Future of Quantum Cryptographic Communications

An interview with two researchers pioneering new frontiers for humanity

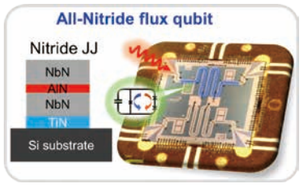






CONTENTS

NICT NEWS 2026 No.5 Vol.519
National Institute of Information and Communications Technology



Cover Photo

Equipment for quantum optics experiments on an optical table (Upper); a compact transmitter installed on the ISS to verify the feasibility of satellite quantum key distribution (Center); and the current configuration of the Tokyo QKD Network operated by NICT (Bottom). These images illustrate the broad, multifaceted scope of research and development aimed at translating laboratory outcomes—including photon generation and control, communications through space, and the long-term operation of metropolitan-area fiber-optic networks—into real-world quantum communications, thereby bringing the technology closer to social implementation.

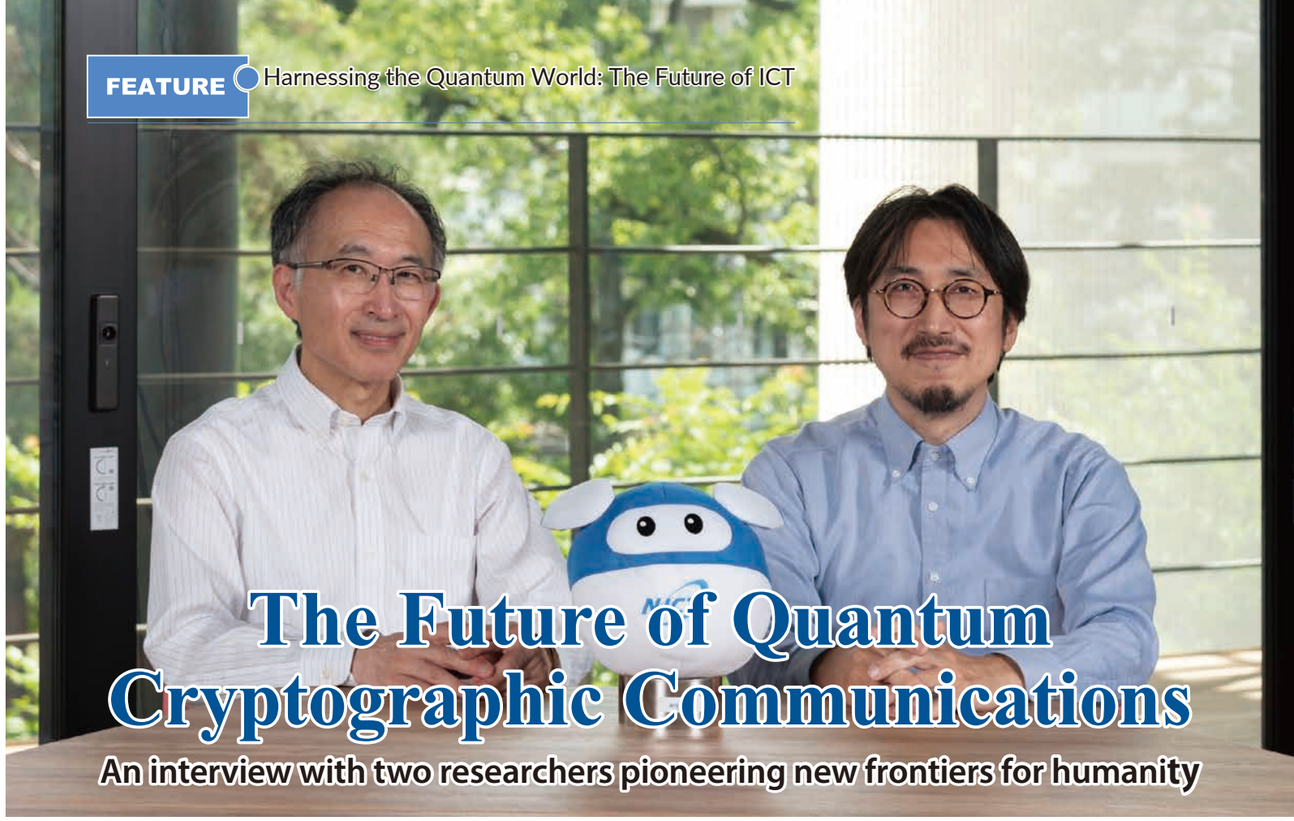
Photo Upper Left

A niobium nitride (NbN)-based superconducting qubit chip coupled to a harmonic oscillator (Right) and the layered structure of the Josephson junction (Left). Fabricated using microfabrication technology, this device provides a platform for the precise control of quantum states.

FEATURE

Harnessing the Quantum World: The Future of ICT

TOPICS



FEATURE Harnessing the Quantum World: The Future of ICT

The Future of Quantum Cryptographic Communications

An interview with two researchers pioneering new frontiers for humanity

TOMITA Akihisa
Director General, Quantum ICT Collaboration Center

After completing graduate school, Dr.TOMITA worked at a corporate research laboratory of a private company and as a university professor before joining NICT in 2025. He is engaged in research on quantum information technology, photonic quantum information processing, and quantum cryptography.
Ph.D. (Engineering).

KATO Go
Research Executive Director of Koganei Frontier Research Center/ Director of the Quantum ICT Laboratory, Advanced ICT Research Institute

After completing graduate school, Dr.KATO worked at a corporate research laboratory of a private company before joining NICT in 2022. He is engaged in theoretical research on quantum control and quantum cryptography.
Ph.D. (Science).

Quantum cryptographic communications is a new technology with the potential to transform the very concept of information security. Based on the principles of quantum mechanics, this innovative technology is expected to find practical applications in a wide range of fields, from national security to business and personal data protection. In this article, we present a discussion between two researchers working at the forefront of quantum communications technology, a field facing ever-intensifying global competition in development: TOMITA Akihisa, Director General of the Quantum ICT Collaboration Center, and KATO Go, Director of the Quantum ICT Laboratory, Advanced ICT Research Institute.

First, could you tell us about your backgrounds?

TOMITA For about 14 years, I was engaged in research on semiconductor-based optical devices for optical communications at a private company. In 1999, I began conducting research on quantum information. In 2010, I joined Hokkaido University, where I conducted experimental research on quantum information and photonic quantum information processing. I joined NICT in April last year and have continued working on quantum cryptography and related areas, with a recent focus on standardization. Since April this year, I have served as Director General, Quantum ICT Collaboration Center, overseeing a broad range of quantum ICT initiatives, including efforts toward social implementation of the technology.

KATO At university, I studied mathematical physics to elucidate physical phenomena through analytical methods. After completing my doctoral program in 2004, I joined a private company, where I became interested in quantum information as a field of theoretical research because of its clear potential for future applications. I have since continued conducting research in this field, including quantum cryptography. In 2022, I joined NICT, and my research focus shifted toward quantum communications, including quantum cryptography. Early in my career, I wanted to achieve results that would make their way into textbooks. Over time, howev-

er, I came to realize that this goal and making a lasting contribution to society could coexist and that both were worth pursuing. Currently, as Director of the Quantum ICT Laboratory, I keep abreast of theoretical developments in quantum cryptography while also overseeing research on quantum information processing.

What is Your View of Modern Internet Society?

TOMITA Our daily lives would be paralyzed without communications. People used to interact only with those within sight, earshot, or running distance. However, communications have expanded these boundaries, increasing the number of people with whom we interact. An environment in which people are connected through communications has become the norm.

KATO When I travel abroad on business, I have no concerns as long as the Internet is available. However, the moment the connection is lost, everything comes to a halt. This says it all. In other words, the Internet is indispensable—something inseparable from our lives.

TOMITA When everyone uses the Internet, we do not know who else is connected or what their intentions may be. Some of them may have malicious intentions. The question, then, is how to block such people. Various technologies have been developed for this purpose, but none is flawless.

KATO Given such circumstances, I believe conducting research in this area is worthwhile. Quantum communications can, in principle, provide certain capabilities and security properties that cannot be achieved through conventional communications alone. Exploring how far we can go using such technologies is valuable for humanity. Taking on the challenge of quantum communications is important as a way of opening up new horizons.

How do you see the Risk of Information Leakage Evolving in the Future?

TOMITA Unfortunately, the risk of information leakage will not diminish. New generative AI models are extremely effective in identifying vulnerabilities in software implementations. In fact, when network software developers tested their own programs using these models, thousands or even tens of thousands of vulnerabilities were identified in a single day. Such models are useful as long as they are used legitimately to identify software vulnerabilities. However, there will always be people who seek to exploit these vulnerabilities. While defensive technologies will continue to advance, some people will certainly try to bypass them, find new loopholes, and profit from them. A cat-and-mouse game of this kind will continue endlessly, with both sides growing increasingly sophisticated.

KATO As long as many people share a system, there will inevitably be some users with malicious intentions. In my view, the process of recovering from such problems resembles biological evolution. Our incessant efforts to overcome shortcomings and build a better-functioning system help humanity mature. Therefore, we should keep making improvements with the mindset that "Such malicious people are helping us grow."

What Aspects of Quantum Communications are Appealing?

KATO A unique aspect of quantum communications lies in its exclusivity. In conventional communications, the same information can be sent to multiple recipients. Quantum communications, however, does not necessarily allow this—a property that forms the security basis of quantum cryptography. If quantum information is sent to A, the same information cannot, in general, be sent to B. The reverse is also true. This exclusivity is a distinctive feature of quantum communications.

TOMITA The world of quantum communications is similar to "monogamy." It creates an exclusive bond that cannot be intruded upon by anyone else.

KATO Any attempt to obtain information from the quantum states can leave detectable traces, and this property forms the basis of quantum cryptography. Quantum information is truly faithful, isn't it? (laughs)

What are NICT's Strengths in the Quantum ICT Field?

KATO NICT covers the entire process from research and development to real-world deployment. While universities often focus on specific areas of research, NICT, with researchers working on a wide range of subjects, makes it possible to engage in discussions with researchers who bring different perspectives. I believe this is NICT's greatest strength.

What has Left the Strongest Impression on you in the Course of Demonstration Experiments and Social Implementation?

TOMITA The most impressive occasion for me was the Tokyo QKD Network experiment in October 2010. QKD stands for Quantum Key Distribution. It is a technology that allows users to share secure cryptographic keys through quantum communications. It was the first practical QKD network built in Japan. QKD devices developed by Toshiba, NEC, and overseas research institutes were connected to build a metropolitan-area network, demonstrating high-speed QKD and video conference secured by QKD-generated key. That was a milestone that marked the beginning of subsequent developments. It was significant in that it demonstrated the viability of the technology as social infrastructure.

KATO When the Tokyo QKD Network was built, it was considered groundbreaking simply to have deployed QKD in the field. It was such an achievement that everyone in this community knew about it.

TOMITA Meanwhile, competition for the development of quantum cryptography has become increasingly intense across the world.

KATO I agree. The environment surrounding quantum cryptography has drastically changed, with global competition to develop the technology intensifying. This makes it necessary for us to seriously consider our raison d'être as an organization and how to communicate it.

TOMITA In terms of where our strengths lie and what we should focus on going forward….

KATO I personally think that it is important to communicate honestly, including openly acknowledging our weak areas in which we need to make greater efforts. I believe we need to do this immediately, as we have counterparts with an overwhelming advantage over us in terms of resources, at least in the field of quantum cryptography.

What Kinds of Obstacles Exist in the Process of Moving from Research to Practical Implementation?

TOMITA One recent example is the certification system used to verify that our QKD devices intended for commercialization are genuinely viable. Certification is crucial because, even if there is demand for these devices, they cannot be adopted unless their security is proven. Building momentum for the adoption of quantum ICT in society is another challenge, requiring many different efforts at each stage. While institutional issues are an immediate challenge, in the long term, we need to develop technologies that are viable for real-world use.

KATO I recently realized that if quantum cryptographic devices cost just JPY 100 per unit, people would readily buy them, experiment with them, and perhaps discover entirely new applications. Therefore, one way of encouraging the adoption of quantum ICT in society would be to make such devices inexpensive. To achieve this, they must be produced in large quantities, which creates a chicken-and-egg situation. Still, I think pursuing low prices could be an effective strategy to promote the social implementation of quantum ICT.

What is the Future of Quantum ICT?

TOMITA The keyword would be the security of quantum communications. The ability to ensure secure communications over extremely long periods of several decades or even hundreds of millions of years is a highly distinctive feature of our current work on quantum cryptography.
My dream is to expand the frontiers of humanity's knowledge. I believe that quantum ICT could open up a new world. I am also certain that it will bring real-world benefits, which will motivate us to advance quantum ICT further. Meanwhile, advancing this technology may drive the development of technologies to harness quantum phenomena and reveal new horizons that we cannot yet see.

KATO I think it comes down to viewing research on quantum ICT from the perspective of what it can offer to the world. Quantum ICT is, in my view, modern alchemy. Alchemy failed in its primary goal of producing gold, yet its research made a significant contribution to the advancement of science. For example, quantum ICT is expected to be useful in areas such as quantum cryptography. However, challenges involving transmission distance and other practical issues remain to be overcome. Some of the applications we currently envision may ultimately prove impractical. Even so, the knowledge gained in pursuing them can have lasting scientific value. Many researchers are currently studying quantum ICT and quantum cryptography, working hard to figure out how to handle things humanity has never dealt with before. This is humanity's frontier. The knowledge gained through this research may open up a new world in the future. In other words, such research may leave a legacy for future generations. Now that we are in an environment where we can create such a legacy, it is important to continue conducting research while periodically reflecting on whether we are truly building that legacy.

Thank you for your time today.

Entanglement Swapping using Sum-frequency Generation between Single Photons

Towards photonic quantum information processing exploiting nonlinear interaction between single photons

TSUJIMOTO Yoshiaki
Research Manager
Quantum ICT laboratory
Koganei Frontier Research Center
Advanced ICT Research Institute

After graduating a doctorial course, Dr.TSUJIMOTO joined NICT in 2017. He has engaged in research on the development of entangled photon-pair sources and the proposal and experimental demonstration of quantum protocols based on such sources.
Ph.D. (Science)

The realization of quantum ICT requires technology that enables the control of photon-photon interactions and precise manipulation of entangled states. Entanglement represents a distinct form of correlation unique to quantum mechanics that cannot be explained by classical physics. Traditionally, quantum operations based on the photon-photon interactions have been indirectly achieved utilizing quantum interference.

On the other hand, if nonlinear optical effects—where multiple light fields interact to generate light at a new frequency—can be realized at the single-photon level, photons can be made to interact directly. This is expected to lead to higher functionality and miniaturization of quantum information processing systems. In this article, we introduce our research results, which demonstrate the world's first application of a nonlinear optical effect between single photons to quantum operations.

Background

In quantum ICT, in addition to operations on individual qubits, the implementation of quantum operations involving multiple qubits will be a key enabling technology. In photonic implementations, such operations have traditionally been realized by using quantum interference between two photons (two-photon interference). In this two-photon interference, as shown in Figure 1(a), a single photon is injected into each of the two input ports of a 50/50 beamsplitter (transmittance = reflectance = 1/2). When the two input photons are distinguishable from each other, the probability of two photons exiting from one output port or of one photon exiting from each output port are both 1/2. On the other hand, when the two photons are completely indistinguishable, the latter event is suppressed due to quantum interference between the photons. A representative quantum communication protocol based on the two-photon interference is entanglement swapping. By connecting two entangled photon pairs, this protocol enables the generation of entanglement between two photons that were originally uncorrelated. Specifically, one photon is taken from each entangled pair to perform a two-qubit measurement called a "Bell-state measurement (BSM)," which utilizes two-photon interference. Through this measurement, new entanglement is generated between the remaining two photons, which originally belonged to different photon pairs. However, the generation of entangled photon pairs is generally probabilistic, which presents a major challenge. As illustrated in Figure 1(b), a successful event, in which one entangled photon pair is generated in each of A1–A2 and B1–B2, occurs with the same probability as a failure event, in which both pairs are generated in one source while no pair is generated in the other. Unfortunately, the BSM based on the two-photon interference cannot distinguish between these success and failure events. Therefore, to confirm the success of entanglement swapping, it is necessary to detect the arrival of a single photon at each of A1 and B2. However, since these photons are destroyed upon detection, the photons resulting from the entanglement swapping cannot be utilized for further applications.

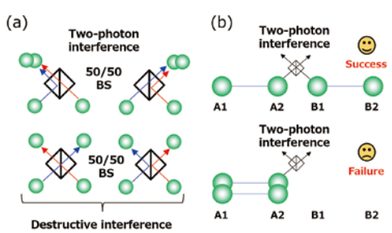


Figure 1 (a) Schematic of two-photon interference
(b) Entanglement swapping by conventional two-photon interference

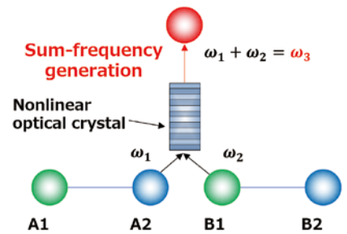


Figure 2 Entanglement swapping using sum-frequency generation between single photons

Single-Photon Nonlinear Optical Effect

As an alternative approach to solve this problem, a new theoretical method of performing a BSM has been proposed (Figure 2). It exploits sum-frequency generation (SFG) between two single photons, rather than two-photon interference. SFG is a nonlinear optical process where new light is generated when two light fields with different frequencies are input into a nonlinear optical crystal. The frequency of the new light equals the sum of the two original frequencies. In this method, as illustrated in Figure 2, photons A2 and B1 are prepared at different frequencies and input into a nonlinear optical crystal. Consequently, only when both photons are present, a photon with the sum frequency is generated. Detecting this SFG photon heralds the successful BSM. The advantage of this method lies in the fact that failure events—such as two pairs being generated at A1-A2, but not at B1-B2—do not result in the generation of an SFG photon. Therefore, this method can eliminate failure events at the BSM stage, which cannot not be distinguished using conventional BSM. Consequently, whenever the BSM succeeds, an entangled photon pair is always obtained. This eliminates the need to destroy the swapped photon pairs. This feature provides a critical advantage for the loophole-free Bell test* and for device-independent quantum key distribution over longer distances.

However, although the first experimental demonstration of such single-photon SFG was reported in 2014, the detection signal of the SFG photon was extremely weak, comparable to background noise. Therefore, to realize entanglement swapping using single-photon SFG, it was necessary to significantly improve the signal-to-noise ratio (SNR) of the SFG-photon detection.

Entanglement Swapping Using Single-Photon SFG enabled by Enhanced SNR

In this study, we constructed an experimental setup that combined NICT's cutting-edge technologies (Figure 3) and achieved the world's first entanglement swapping using single-photon SFG. The experimental process is as follows: First, two entangled photon pairs were generated. Next, one photon from each pair was input into a periodically poled lithium niobate (PPLN) waveguide to create an SFG photon. Then, a superconducting single-photon detector (SSPD) was used to detect the SFG photon. This heralds the successful completion of entanglement swapping, leaving the remaining two photons in an entangled state. For this experiment, the following specific technologies were utilized. First, to maximize nonlinear optical efficiency, a long PPLN waveguide with a crystal length of 63 mm was fabricated. This long PPLN waveguide was then placed inside a Sagnac interferometer to achieve two-qubit operation. The generated SFG photons were detected by a low-noise SSPD, specifically a dark count rate of 0.15 Hz. Furthermore, we used an electro-optic comb to generate the pump pulses for the entangled photon-pair source at a high repetition rate of 1 GHz, optimized for the present experiment. Through the above technologies, we were able to achieve an SNR for the SFG photon detection that was nearly an order of magnitude higher than in previous studies (Figure 4(a)). Figure 4(b) shows the polarization correlation of the photon pairs obtained through the entanglement swapping. From the average contrast value of the experimental data, the lower bound of the fidelity to the maximally entangled state was estimated to be 0.770 ± 0.076. This value confirms the first realization of entanglement swapping using nonlinear optical effect between single photons. The results obtained from this study represent a major step forward in photonic quantum information processing. In the future, this is expected to become a key technology for generating entangled photon pairs on demand.

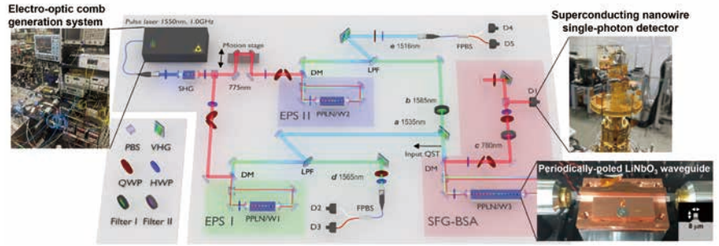


Figure 3 Demonstration of entanglement swapping using sum-frequency generation between single photons. EPS I and EPS II each generate an entangled photon pair, and an SFG-BSA (Bell-State Analyzer) performs a BSM using sum-frequency generation between the single photons.

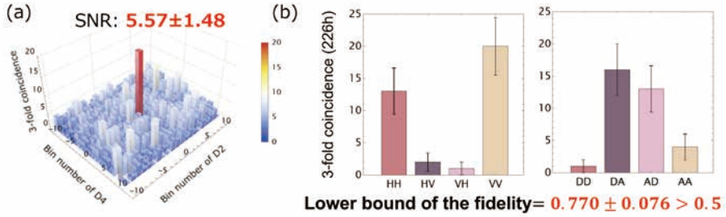


Figure 4 (a) The three-fold coincidence among D1, D2 and D4. (b) Polarization correlation of the two photons after the completion of entanglement swapping. H, V, D, and A represent horizontal, vertical, diagonal (+45°), and anti-diagonal (-45°) polarizations, respectively.

Future Prospects

We expect that further improvement in the SNR will be necessary to apply our methodology to more advanced quantum information protocols than entanglement swapping. For example, our simulations indicate that the nonlinear effect needs to be improved by at least a factor of three for the loophole-free Bell test, and by a factor of 50 for device-independent quantum key distribution. We aim to enhance the nonlinear optical effects, leading to the development of more efficient and compact photonic quantum computing circuits, as well as next-generation quantum key distribution over longer distances.

* Measuring the correlations of entangled photon pairs violates Bell inequalities, which hold under the assumptions of locality and realism. However, if only a small fraction of the generated entangled photon pairs is detected, a loophole arises. We cannot rule out the possibility that the inequalities would hold true if the undetected pairs were also taken into account (the detection-efficiency loophole). Detecting sum-frequency-generation photons enables a verification experiment that closes this loophole.

Towards the Realization of Satellite Quantum Key Distribution

Experiment on key sharing between the International Space Station (ISS) and a ground station

FUJIWARA Mikio
Distinguished Researcher
Quantum ICT Collaboration Center
Dr. FUJIWARA joined the Communications Research Laboratory (Currently NICT) in 1992.
He has engaged in research and development of far-infrared detectors, quantum key distribution, and quantum secure cloud.
Ph.D. (Science)

OZAWA Shunsuke
Senior Researcher
Quantum ICT Laboratory
Koganei Frontier Research Center
Advanced ICT Research Institute
Dr. Ozawa had engaged in observational research on high-energy cosmic rays at the University of Tokyo and Waseda University.
He Joined NICT in 2019. Since then, the research on satellite quantum cryptography became the research topic.
Ph.D. (Engineering)

Quantum computer development is currently being actively pursued by many countries around the world.

Quantum computers hold the potential to process extremely complex calculations in a fraction of the time required by conventional supercomputers, which would otherwise take thousands of years. Driven by this remarkable computational capability, innovative breakthroughs are anticipated across a broad spectrum of fields, including acceleration of drug discovery, optimization of logistics and power generation systems, and advanced financial risk analysis. On the other hand, there are growing concerns that standard cryptographic algorithms widely used on the Internet (such as public-key cryptography) could eventually become vulnerable to attacks by future large-scale quantum computers. Consequently, there is an urgent need for novel defense technologies that can ensure secure communications even after quantum computers become practically available. Quantum key distribution represents one of the most promising technologies to resolve this challenge. To enable its global network, we are advancing research and development to integrate QKD system onto satellite platforms.

Quantum Computers and Quantum Cryptography

Quantum technology leverages the unique physical properties exhibited by microscopic entities such as photons, electrons, and atoms, including superposition and quantum entanglement, to achieve ultra-high-speed computation, ultra-sensitive measurement, and unconditionally secure communications that far surpass conventional capabilities. In recent years, countries around the world have been actively developing quantum computers that can utilize the superposition property of quantum states to rapidly compute optimal solutions among an immense number of combinations. In addition to national projects, major companies with massive capital are competing to develop quantum computers with the expectation that they will be applied to drug discovery, materials science, and logistics optimization. However, the societal impact of quantum computers is not limited to these positive applications. With quantum computers, encryption schemes currently relied upon to safeguard our daily Internet communications may become vulnerable to instant decryption. Even if an attacker cannot decrypt data immediately, a critical threat scenario involves storing intercepted ciphertext now and decrypting it all at once after a quantum computer has been fully realized. Today's Internet routinely transmits data requiring ultra-long-term confidentiality, such as personal genomic data. Mitigating the risk of information leaks caused by the advent of quantum computers is therefore a pressing necessity.

This attack methodology—storing intercepted data now for future decryption—is known as a "Harvest Now, Decrypt Later" (HNDL) attack, and developing countermeasures against it has become an urgent global priority. "Quantum cryptography" has drawn significant attention as an effective remedy for Harvest Now, Decrypt Later attacks. It combines Quantum Key Distribution (QKD), which can invariably detect eavesdropping attempts and allows two distant parties to accomplish a secure secret key agreement, with Vernam's One-Time Pad (OTP) cipher, which encrypts information bit by bit using the key. This combination enables encrypted communications that cannot be cracked by any future super-high-performance computer, regardless of its computational power. Currently, various nations are advancing QKD device research and moving toward practical deployment of QKD devices within public infrastructure.

Tokyo QKD Network Led by NICT

In Japan, a research team led by NICT began researching quantum cryptography in the early 2000s. In 2010, NICT began operating the "Tokyo QKD Network," a networked set of QKD links, which remains operational to this day. To the best of our knowledge, this network represents the longest-running QKD network in the world. NICT has conducted social implementation experiments using this network in collaboration with various private companies and government agencies, successfully developing advanced secure-communication applications.

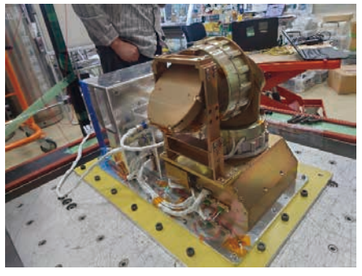


Figure 1 Light source unit for physical layer cryptography and the periscope telescope mounted on the ISS (SeCRETS)

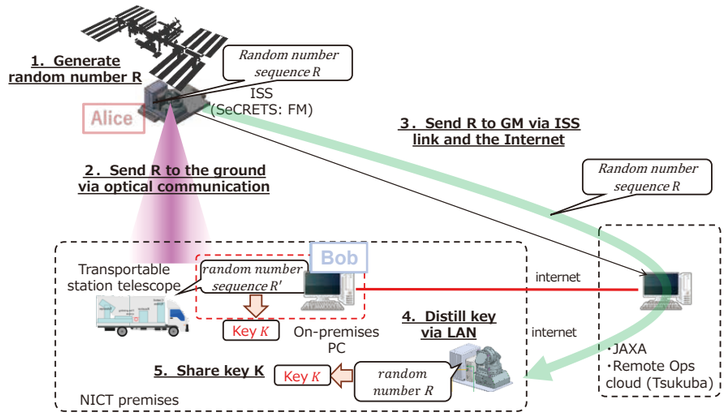


Figure 2 Overall configuration of the physical layer cryptographic communication experiment between the ISS and the transportable optical ground station

Furthermore, equipping artificial satellites with QKD devices makes it possible to realize secure secret key agreement on a global scale.

Development of Satellite Quantum Key Distribution System in Other Countries

Development of satellite-based QKD has also progressed internationally, with China initially taking the lead. In 2017, China launched Micius, the world's first quantum communications satellite, successfully demonstrating secure secret key agreement over an ultra-long distance exceeding 12,000 km.

Meanwhile, in Japan, NICT initiated the development of satellite-borne QKD system in 2018. NICT proceeded with the development of a QKD transmitter capable of being mounted on small satellites, along with a transportable optical ground station that can be carried on an 8-ton truck. Although budget constraints at the time prevented us from launching an independent satellite, NICT advanced technological developments targeted at optical transmission between the International Space Station (ISS) and ground stations. In addition to standard QKD, NICT implemented physical layer cryptography on these devices by leveraging the direct line-of-sight communication channel between the satellite and the ground, enabling even more efficient and secure key generation than standard QKD. In QKD, encryption keys can be shared securely over a photon transmission path even under the assumption that physical operations on quantum memories or quantum computers along the link are permitted. In direct satellite-to-ground communications, appropriate methods can be applied to confirm that no powerful eavesdropper is physically present within the transmission channel. For instance, North American Aerospace Defense Command (NORAD) monitors space and airspace around North America 24 hours a day, 365 days a year using radars and satellites. NORAD has the capability to detect objects 10 cm or larger within its monitored domain. Alternatively, the satellite link can be monitored by telescopes or other surveillance equipment.

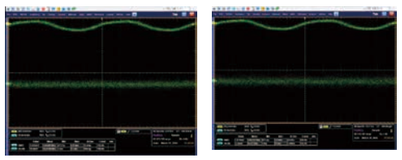
If we accept the prerequisite that "no powerful eavesdropper can invade the transmission path," the scope of eavesdropping risk is reduced to assuming that an eavesdropper can only intercept stray or scattered light that leaks from the satellite-to-ground optical beam.

In this scenario, a final, secure key can be extracted by estimating the upper bound of the leaked information and eliminating the corresponding data. To conduct demonstration experiments of this physical layer secret key agreement between the International Space Station (ISS) and a ground station, NICT developed a light source for physical layer secret key agreement system, a processing unit for key generation, and a transportable ground station in collaboration with Sony Group (Sony CSL), SKY Perfect JSAT, and the Next-generation Space System Technology Research Association (NeSTRA). Figure 1 shows a photograph of the light source unit mounted on the ISS (Secure Laser Communications terminal for LEO: SeCRETS). The periscope-style telescope equipped on the unit can direct its optical axis anywhere in the upper hemisphere. This unit was mounted on the ISS's IVA-replaceable Small Exposed Experiment Platform (i-SEEP) and operated in space. Figure 2 illustrates the overall conceptual architecture of this research. A Differential Phase Shift Keying (DPSK) signal with a 10-GHz clock is emitted from the transmitter on the ISS and received by a 35-cm diameter reflective telescope mounted on an 8-ton truck. Figure 3 shows a photograph of the ground station unit, and Figure 4 displays the received signal waveform. By applying error correction and privacy amplification to the received signal (as a process to securely extract cryptographic keys), we successfully generated over 1 million bits of secure cryptographic keys during a single overhead pass in 2024. Furthermore, we successfully demonstrated OTP-encrypted communications with the ISS.

Figure 3 Transportable optical ground station

Imaging by the guide camera on the telescope in the transportable station

Imaging by the camera on the precision tracking optical system and beacon detection by the QD (Quadrant Detector)



Captured 10-GHz weak optical signals → Successful secure secret key agreement through error correction and privacy amplification

Figure 4 Signal received from the ISS

Future Prospects

Based on the expertise gained through this research, NICT is serving as the lead institution to promote the project, "Research and Development of Small LEO Satellite Enabling Information-Theoretically Secure Key Sharing" using the Space Strategy Fund Program.

Japan's first quantum key distribution satellite, named "N-QUADIS," is scheduled for launch in 2029. Utilizing this satellite, we are conducting research and development aimed at successfully demonstrating technologies for global-scale secure secret key agreement.

Demonstration of a New "Superconducting Flux Qubit" That Requires No External Magnetic Field

New Technology to miniaturize the flux qubit circuit with π junction

Sunmi Kim
Quantum ICT Research Laboratory, Koganei Frontier Research Center Advanced ICT Research Institute Senior Researcher
After completing graduate school, Dr. Kim served as a postdoctoral researcher at the National Institute for Materials Science (NIMS) and Osaka University, and as a project assistant professor at the Institute of Industrial Science, the University of Tokyo. She joined NICT in 2018 and has been engaged in research on superconducting qubits.
Ph.D. (Science).

Quantum computers have the potential to completely change our lives. At the heart of these machines are tiny components called "quantum bits" (qubits), which process information. A joint research team, including NICT, has successfully operated a new type of qubit called a "superconducting flux qubit" at its best performance in absolute zero magnetic field—meaning no external magnetic force is needed at all. This marks a world-first achievement and a major step forward toward making quantum computers smaller and more powerful.

Background

Quantum computers are expected to solve incredibly complex calculations in a flash—tasks that would take today's computers many years to complete. Scientists around the world are researching this technology, hoping it will help develop new medicines and design advanced materials for the future.

Currently, the most widely developed type is the "superconducting qubit," which takes advantage of "superconductivity"—a phenomenon where electrical resistance drops to zero at extremely low temperatures. However, the most popular model used today (the transmon qubit) has a low level of a property called "anharmonicity". This means that when many of these qubits are packed together, their frequencies tend to overlap and cause interference, leading to errors—a problem known as "frequency collision".

On the other hand, "flux qubits," which store information based on the direction of circulating superconducting currents, have high anharmonicity and can reduce this frequency collision problem. Yet, they had a different challenge: to work properly at their best performance, they always needed an external coil to constantly apply a specific magnetic field equal to half a magnetic flux quantum. This required extra bulky parts and complex control wiring for each qubit, creating a massive barrier to building large-scale quantum computers.

The Secret Behind No Magnetic Field: A Tiny Trick with "Ferromagnets"

To overcome this obstacle, the research team focused on a method to shift the phase of the superconducting wave function by exactly 180 degrees (π) without using any external magnetic fields. This intrinsic phase shift is equivalent to applying a half flux quantum to the qubit loop. We achieved this by inserting a special connection called a "π-junction" into the circuit (Figure 1). This junction has a structure where an incredibly thin layer of a magnetic material called a ferromagnet, specifically "PdNi" (palladium-nickel), is sandwiched between two superconductors.

In a standard flux qubit, a specific external magnetic field is required to establish an optimal operating point that is robust against flux noise. At this point, the clockwise and counterclockwise current become completely equal in energy, forming the quantum superpositions that define the |0> and |1> states. While conventional designs relied on large outer coils to precisely apply this magnetic field, the newly developed qubit achieves this intrinsically. The built-in ferromagnet functions as a π-phase shifter for the qubit (Figure 1(a)). As a result, the qubit naturally reaches its optimal operating point when the external magnetic field is exactly zero, successfully eliminating the need for bulky coils and complex control wires.

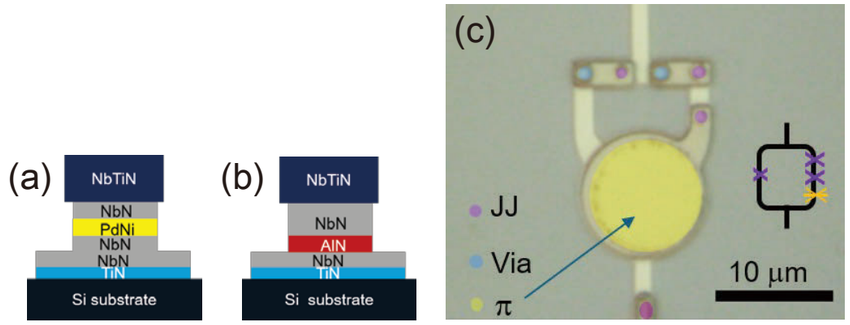


Figure 1 (a) Schematic diagram of the actual nitride-based π-junction.(b) schematic diagram of all nitride Josephson junction (NbN/AlN/NbN) used a basic junction of flux qubit (c) Optical microscope photograph of the actual flux qubit made of nitride, featuring a π-junction (π).

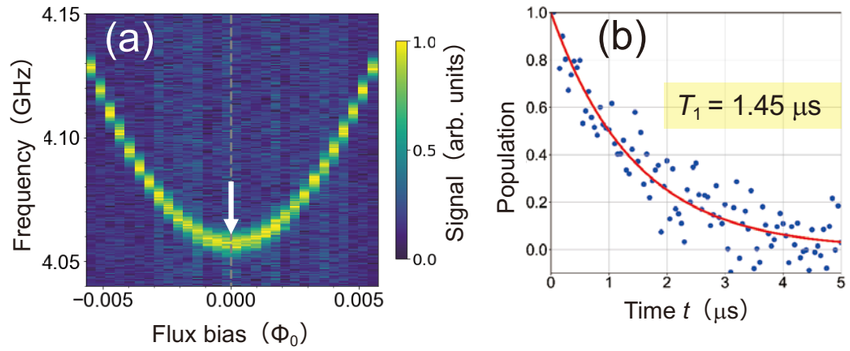


Figure 2 (a) Microwave spectroscopy spectrum showing the magnetic field dependence of the transition frequency from the ground state to the excited state for the nitride flux qubit with a π-junction. (b) Measurement result of the coherence time, showing an energy relaxation time of T1 = 1.45μs.

Improving Qubit Lifetime by employing Nitride Technologies

Previous studies have attempted to incorporate magnetic materials into circuits to eliminate the need for external magnetic fields. However, the lifetime (coherence time) of those qubits was extremely short—only about 4 nanoseconds (10^{-9} second). This limitation was primarily due to the inherently short coherence time of the phase qubit architecture used in those experiments—typically on the order of nanoseconds—rather than any negative influence from the π-junction itself.

In this new study, the team combined NICT's long-standing expertise in growing high-quality crystals of a special superconductor called niobium nitride (NbN) on silicon substrates, NTT's advanced design and measurement techniques for long-lived qubits, and the π-junction expertise from Tohoku University and Nagoya University. The actual device is microscopic in scale, as seen under a microscope (Figure (c)).

By using ferromagnetic materials with a smaller spin-flip scattering and optimizing the circuit layout, the team successfully observed a microwave spectrum demonstrating the qubit's optimal operation in a zero magnetic field (Figure 2(a)). Furthermore, they extended the qubit's lifetime to 1.45 microseconds (μs:10^{-6} second), which is about 362 times longer than previous π-junction phase qubits (Figure 2(b)). This achievement successfully proved to the world for the first time that a flux qubit can operate reliably in a zero magnetic field.

Future prospects

This breakthrough represents the world's first successful demonstration of a novel flux qubit that requires no external magnetic field while achieving a lifetime in the microsecond range. This technology paves the way for vastly simpler, microscopic quantum circuits, laying a solid foundation for packing thousands of qubits onto a single chip in the future.

Moving forward, the research team will continue to optimize the fabrication processes to extend the qubit's lifetime even further and improve fabrication techniques to ensure uniform performance across all qubits. By building a brand-new quantum hardware platform that surpasses the performance of traditional aluminum-based qubits, this technology is expected to accelerate the realization of fault-tolerant quantum computers, bringing them out of the lab and closer to our everyday lives.

Demonstrations for the Social Deployment of Quantum Cryptographic Networks

Realizing everlasting secure communication

TOMITA Akihisa
Director General,
Quantum ICT Collaboration Center

After completing graduate school, Dr.TOMITA worked at a corporate research laboratory of a private company and as a university professor before joining NICT in 2025. He is engaged in research on quantum information technology, photonic quantum information processing, and quantum cryptography. Ph.D. (Engineering).

Due to technological advancements, currently cryptography may be compromised in the future, creating a need for cryptographic algorithms that can guarantee long-term security. For this reason, quantum key distribution (QKD), which is based on quantum mechanics, is attracting significant attention. NICT has developed QKD platforms and quantum secure clouds and has been verifying their practicality. In the future, the development of hybrid systems combining QKD networks with post-quantum cryptography and the realization of the quantum Internet including satellite QKD and quantum relays are anticipated.

Background

In today's society, a wide variety of information is exchanged among people distant from each other. It is cryptography that supports trust in the integrity and security of the information exchange. The key that is used to retrieve information is the most critical element in cryptography. A key is an unpredictable random number sequence, which should be kept confidential. In the cryptographic systems widely used today, a key is given as a solution to a mathematical problem that is difficult to solve even for a powerful computer. Cryptography that is undecipherable in this sense is referred to as computationally secure. However, the mathematical problem can be solved if an efficient solution is discovered or the performance of computers is improved. For this reason, cryptography methods have a lifespan of typically 20 to 30 years to be replaced with new-generations. Even ciphers that are currently secure may be cracked in a few decades, and are vulnerable to attacks called Harvest Now, Decrypt Later (HDNL), a strategy through which attackers intercept and store encrypted information to decrypt in the future when computers are sufficiently powerful.

Seeking Cryptography with Long-term Security

About 30 years ago, it was found that the mathematical problems used for current cryptography would be easily solved by quantum computers. The development of quantum computers has been advancing rapidly in recent years, and it is even predicted that current cryptographic algorithm will be cracked by 2030. Accordingly, research and development are proceeding on algorithms that use mathematical problems even quantum computers cannot solve efficiently (post-quantum cryptography). In the United States, selection of recommended algorithms is being carried out by the government. However, as post-quantum cryptography also has a lifespan, it cannot assure long-term security against HNDL attacks.

Another secure encryption method exists. This method guarantees security by theoretically limiting the amount of information that could be acquired by eavesdroppers. This is called information-theoretic security, which guarantees long-term security even if technologies advance. However, for the practical implementation of information-theoretic secure cryptography, it is necessary to establish an efficient method for sharing common secure keys between the sender and receiver because the cryptographic protocol requires a large number of common keys. Quantum key distribution (QKD) is one such method. The combination of information-theoretic secure cryptographic algorithms and quantum key distribution (QKD) is generally referred to as quantum cryptography.

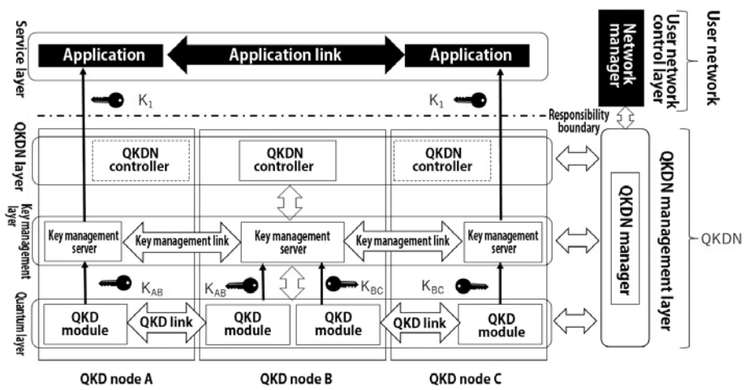


Figure 1 QKD platform configuration diagram

The security of QKD is based on the laws of quantum mechanics. Eavesdroppers observe the quantum state to obtain the key information. However, the state changes unless an appropriate measurement basis is used. Therefore, a trace of eavesdropping appears as an error in the receiver's measurement outcome. The number of errors indicates the amount of information eavesdropped. Creating a key by subtracting the eavesdropped information from the original receiver's measurement result enables the sharing of a key of which the eavesdropper does not have information.

Quantum Key Distribution Platform

As QKD only provides the sender and receiver with a shared secure key, it is necessary to implement functions such as controlling the shared key amount, managing the stored key, and distributing keys to applications. Therefore, NICT has developed a QKD platform. As shown in Figure 1, the platform consists of three layers: quantum layer, key management layer, and (network) control layer. The quantum layer shares keys through QKD. The key management layer distributes private keys to the nodes where keys are required. The control layer issues directions to nodes at the quantum and key management layers. Devices at the application layer receive and use keys. Since key generation and distribution using QKD are completed in the lower three layers, developers can create and run applications at the top layer without even being aware that quantum technology is being used. The Tokyo QKD Network, launched in 2010, has the world's longest operation history as a QKD platform in a metropolitan area and has successfully provided keys to various IT devices such as drones, smartphones, and network switches, successfully supporting confidential communication.

Furthermore, secret sharing is employed for data storage and processing. Secret sharing involves dividing information and storing it across multiple data servers. Even if one server is attacked, the secret remains secure as long as the majority of the other servers remain intact. Additionally, data can be restored even if some servers go down due to a disaster or other cause. While secret sharing is information-theoretically secure, it does not provide confidentiality in data exchange between users and servers. A combination of secret sharing and quantum cryptography enables information-theoretically secure data transmission, storage, and processing. NICT is the first in the world to propose and demonstrate such a system as a quantum secure cloud. In collaboration with companies in Japan, proof-of-concept experiments have been conducted on systems such as one that stores genome data and transmits it between a genome research center and hospitals by using quantum cryptography, another system that transmits facial recognition feature data confidentially , and a third that encrypts electronic health record data with QKD keys and transmits it securely over a network from a decentralized backup system. In addition, NICT has also succeeded in combining a quantum computer and quantum secure cloud. Users send data stored in the quantum secure cloud to the quantum computer and receive analysis results. Valuable data exchanged can be protected using quantum cryptography.

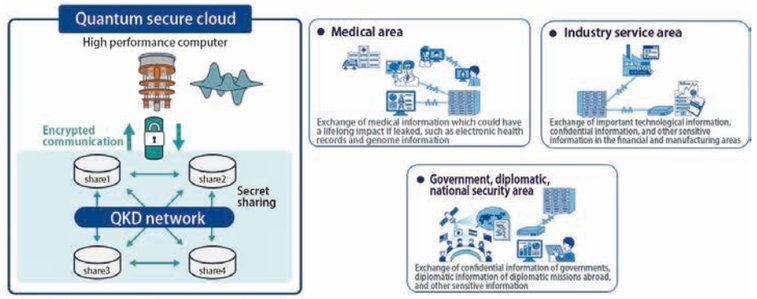


Figure 2 Quantum secure cloud and application areas

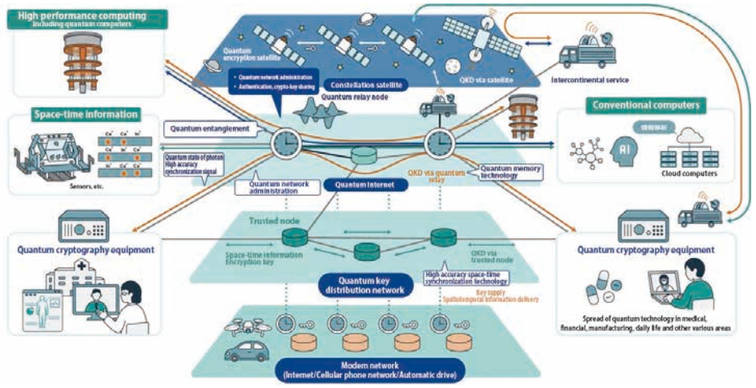


Figure 3 Future of quantum Internet

As such, quantum-secure clouds are expected to find applications in the medical, defense, finance, government, and critical industrial infrastructures, where information must remain confidential for decades or more to withstand HNDL attacks (Figure 2).

Future Prospects

Quantum cryptography entails higher costs and has a more limited range of applications compared to post-quantum cryptography. It is necessary to develop a hybrid cryptographic system that combines the advantages of post-quantum cryptography and quantum cryptography and to properly position and implement each within social infrastructure. In addition, as global network, integration with satellite-based quantum key distribution, as well as research and development on quantum relay technology for the future are also important. It is anticipated that the quantum Internet, which will integrates quantum cryptography, modern cryptography, quantum computers, quantum sensors, and optical and wireless communications networks, and other relevant technologies will be realized (Figure 3).

Watch Now! Let's Learn Through Super Easy Animation "The World of Quantum"

Assistant Chief, General Planning Office, Quantum ICT Collaboration Center **YASUI Yuri**

NICT has released an animated video titled “Let's Learn Through Animation! The World of Quantum” on its official YouTube channel. The video explains basic quantum concepts in an easy-to-understand way.

In recent years, terms such as quantum computing and quantum cryptographic communications have increasingly appeared in the news. Research and development on these technologies is being conducted around the world, as they are expected to support next-generation information-processing and communication technologies. Still, many people are probably wondering, “What exactly is a quantum?”

This video, co-created by the Quantum ICT Collaboration Center and the Quantum ICT Laboratory, is designed to help viewers intuitively understand the basic concepts of quantum physics. Set in a science classroom or a laboratory in the near future, the video features Yoko, a researcher, and high school students Sora and Nami. Through their conversations, they explain basic quantum concepts and the fields of quantum research being pursued at NICT in clear and easy-to-understand terms.

Animation’s unique visual techniques allow viewers to learn about the mysterious properties of invisible quantum phenomena in an enjoyable way. The content is accessible not only to those who are interested in quantum, but also to those who are learning about it for the first time.

In addition, popular voice actor KAYANO Ai voices Yoko in the video. The characters’ conversations make the quantum world feel more accessible to viewers.

With only 101 years having passed since the birth of quantum mechanics, our exploration of the quantum world has just begun.

We hope this video helps spark viewers’ interest in and deepen their understanding of quantum technologies that will shape the future.

Watch “Let's Learn Through Animation! The World of Quantum” on NICT’s official YouTube channel and take a peek into the intriguing quantum world.

“Let's Learn Through Animation! The World of Quantum” on NICT’s official YouTube channel:
URL: https://www.youtube.com/watch?v=2dJyYo2H9Pw (Japanese Version)

Research and Development of Fundamental Technology for Increasing the Reliability and Efficiency of Satellite-based Quantum Key Distribution

KAWASHIMA Teruyoshi
Tenure-Track Researcher, Quantum ICT Laboratory, Koganei Frontier Research Center Advanced ICT Research Institute, Ph.D. (Science)

Biography

1998 Born in Chiba
2021 Graduated from the Department of Physics, Faculty of Science and Technology, Keio University
2026 After completing the doctoral program at the Graduate School of the University of Tokyo, joined NICT and assumed the current position

AWARDS

2022 Received the Student Presentation Award of the Physical Society of Japan 2022 Autumn Meeting

Q&As

Q What is the best thing about being a researcher?
A I have aspired to be a researcher since childhood, so I am truly glad to be able to work in research from now on. At NICT, especially, I find it rewarding that I can pursue my own interests while also returning the achievements to society.

Q Things you are into right now
A I enjoy taking a walk in the premises of NICT with members of the Quantum ICT Laboratory after lunch, observing plants and insects. The photo shows a rare plant named "golden orchid" which grows only where it has the appropriate symbiotic relationship with soil fungi and trees and is difficult to transplant.

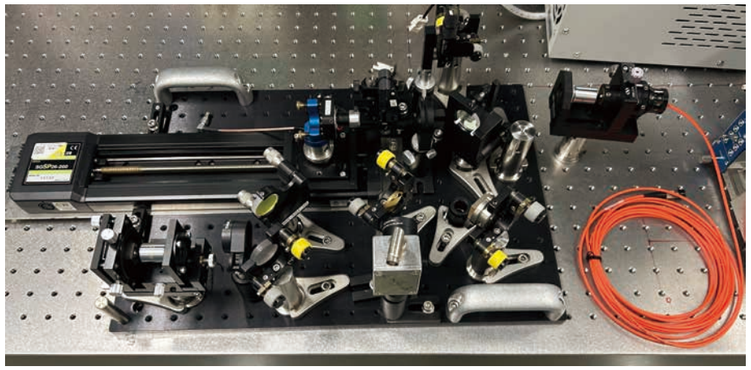
Q How do you spend your days off?
A On my days off, I work out at a gym, explore the food scene in my neighborhood such as ramen, and the like. I sometimes go on a trip or go to a live music concert. The photo is from when I went to a live concert of ”back number" with my family.

At graduate school, I participated in an air shower experiment that observed high-energy cosmic rays, and I was engaged in photodetector development and data analyses. For the photodetector development, I improved the readout circuit of the photomultiplier tube and developed a detector system that was capable of measuring signals with a wide range of intensities. In addition, I was also engaged in research involving the analyses of the distribution of cosmic ray arrival directions based on observation data for examining the anisotropy of cosmic rays.

From now on, leveraging my experience in detector development and the expertise I gained through the cosmic ray research, I will be engaged in research aiming at the practical implementation of satellite-based quantum key distribution (QKD).

The Quantum ICT Laboratory is focusing its efforts on globally expanding the QKD ground fiber network through satellite-to-ground optical communications technology. Satellite onboard equipment is required to be resistant to the space environment as well as small sized, light weight, and low power consumption. Because QKD uses a transmission protocol based on polarization modulation, satellite onboard cryptography equipment consists of a special interferometer, LN modulator, and other components. I would like to integrate their functions to develop a QKD transmitter that is small in size, has low power consumption, and works stably even in a satellite orbit.

On the other hand, ensuring the safety of quantum communication of satellite onboard equipment is a critical issue for social implementation. Although QKD transmission equipment is required to transmit "independent and identically distributed" photons, standard methods for measuring and analyzing the polarization, correlation, and temporal fluctuations of bit sequences and optical signals have not been established. For this reason, safety verification of not only satellite onboard equipment but also ground QKD is demanded. Because this issue is closely related to transmitter development as well, I would like to conduct them concurrently. Through these efforts, I will increase the reliability and safety of QKD equipment, thus contributing to the realization of practical satellite quantum communications systems.



Building an optical system (1-bit delay line interferometer) for evaluating the existence of correlation between bits, aiming at safety verification of QKD

NICT NEWS 2026 No.5 Vol.519
Published by **Public Relations Department, National Institute of Information and Communications Technology**
Issue date: Sep. 2026 (bimonthly)

4-2-1 Nukui-Kitamachi, Koganei, Tokyo
184-8795, Japan
E-mail: publicity@nict.go.jp

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

ISSN 2187-4050 (Online)