NICT National Institute of Information and Communications Technology

QUANTUM NETWORK WHITE PAPER

2021 —— 2035

Quantum Network White Paper

(0.9 version)

National Institute of Information and
Communications Technology (NICT)
April 2021

Table of Contents

Chapter 1: Introduction

1. About the White Paper

(1) Objective

・At present, efforts are underway in Japan and overseas to develop quantum cryptography and quantum networks (the ultimate goal is the ”Quantum Internet”). In January 2020, the Japanese government released the ”Quantum Technology Innovation Strategy.” NICT has been promoting cutting-edge R&D related to quantum networks. In addition, NICT, as the ”Quantum Security Hub” in the Strategy, started promoting to create a hub for industry-academia-government collaboration and to develop human resources from FY2020.

・By releasing this white paper, we would like to show the direction of NICT's research and development as the hub of quantum security and the issues to be tackled in the future, to attract international researchers, to promote cooperation with international research institutes, and to accelerate research and development toward quantum networks.

(2) Overview of the white paper

・This white paper consists of international trends of quantum communication, the image of society and use cases to be realized by quantum networks, the R&D roadmap and promotion strategy that NICT will work on to realize the society and the use cases. This white paper is published as the first edition.

・The ultimate goal of this white paper is the ”Quantum Internet”. In order to understand the importance of collaboration among various stakeholders in Japan and overseas, as well as research and development efforts, this paper is intended for virous readers, including governments, companies, universities, and research institutions.

(3) Discussion team and schedule

・This white paper was the result of discussions among NICT researchers in the fields of quantum ICT, future ICT, space communications, and networks, as well as NICT officials working on the promotion of quantum networks, over a period of 5 months from November 2020 to March 2021.

2. International trends and the overview of quantum information communications

(1) Overview of quantum information communications

・Information and communications technology, such as the Internet, supports the development of the world's economy and society, and is a source of industrial competitiveness.

At present, we are in the midst of digital transformation (DX) in COVID-19 pandemic, and the social change is progressing by utilizing information and communications networks.

・On the other hand, cyber-attacks on information and communications networks continue to increase, and the realization of safe and secure information and communications infrastructure is required.

・It is feared that modern cryptography used in modern information and communications networks will be compromised by the high performance of quantum computers being developed by major IT companies in the United States. The National Institute of Standards and Technology (NIST) in the United States is investigating and evaluating post-quantum cryptography. It is also feared that there will be an attack in which encrypted data flowing through the current information and communications networks are eavesdropped/obtained, and then decrypted when a high-performance quantum computer is put into practical use (harvest now, decrypt later).

・For this reason, quantum cryptography is required as a technology to realize "information-theoretic security" that is impossible to decrypt by any computer in principle. Several countries such as the United States, Europe, and China, including Japan, are rapidly promoting R&D, demonstration for practical application, and construction of quantum cryptography networks for actual operation.

・The Beyond5G/6G, for which R&D activities have started in various countries around the world, has "ultra-security and reliability" as one of its functional requirements, and quantum cryptography is expected to play an important role here as well.

・Research and development of quantum computing and quantum sensing technologies are currently underway in Japan and overseas. In the future, it is expected that these technologies will be put into practical use and connected to quantum networks, enabling ultra-large-scale information processing and ultra-high-precision information collection (see Chapter 2). Basic research is being conducted in Europe and the United States with the aim of creating so-called the "Quantum Internet," in which quantum information devices are connected to quantum networks.

・ The quantum internet is expected to become a new social infrastructure by realizing new applications and services that have never been seen before. Research and development of quantum networks and efforts to implement quantum networks in society have become important initiatives that are directly linked to ensuring national economic and social prosperity and national security.

(2) Policies and R&D trends regarding quantum ICT

・ Foreign countries such as the United States, Europe, and China have formulated R&D strategies for quantum information communications, including quantum key distribution and quantum networks, as strategic core technologies, and are making large-scale R&D investments. In addition, these countries are promoting strategic initiatives such as forming R&D hubs and developing human resources.

① Policy and R&D trends in the United States

・ In the United States, based on the "National Initiative Act" (2018), the Department of Energy (DOE) and the National Science Foundation (NSF) are investing $1.2 billion over five years in research and development of quantum information science from a long-term perspective on a science-first approach. In this context, the DOE and the NSF are collaborating with universities, companies, and other organizations to promote research, development, and demonstration of elemental technologies and human resource development for the realization of the quantum internet. The Office of Science and Technology Policy (OSTP), in its ”Strategic Vision for U.S. Quantum Networks” (February 2020), has identified six areas of research activity that should be targeted and focused on for the quantum internet, as well as goals for the next five and 20 years. The DOE held “Quantum Internet Blueprint Workshop” (July 2020) to discuss the direction and milestones of research and development for the quantum internet.

② Policy and R&D trends in Europe

・In Europe, the European Commission has pledged to invest € 1.0 billion over five years in the ”Quantum Flagship” (since 2018) to conduct R&D on quantum technologies. In March 2020, the European Commission released the “Strategic Research Agenda on Quantum Technology” with the ultimate goal of the quantum internet, which includes a roadmap for R&D, industrialization, standardization, and human resource development. In addition, 25 countries in Europe have agreed to develop a quantum communication infrastructure, “EuroQCI”, which would lead to the construction of the quantum internet network. In addition, the Commission is promoting the construction and demonstration of a QKD testbed through the “OpenQKD” project.

・European governments, including the United Kingdom, Germany, and France, are also promoting R&D of elemental technologies for QKD and the quantum internet.

③ Policy and R&D trends in China

・In China, a quantum cryptography communication backbone connecting Beijing and Shanghai and metropolitan area networks in major cities have been constructed. The total length of the quantum cryptography networks have reached more than 7000 km as of 2018. A number of companies have been established to provide communication equipment, devices, and platforms. In addition, China launched the ”Mozi” satellite in 2016 and successfully demonstrated a quantum cryptosystem between the satellite and the earth. In January 2021, China released to conduct a demonstration of an integrated quantum network between a satellite and the ground to promote the deployment of an integrated quantum cryptography network across China.

④ Policy and R&D trends in Japan

・In Japan, in 2018, the Cabinet Office launched the second phase of the Strategic Innovation Program (SIP), the Ministry of Education, Culture, Sports, Science and Technology launched the Optical and Quantum Leap Flagship Program (Q-LEAP), the Ministry of Economy, Trade and Industry launched quantum computing (quantum annealing computer, etc.), and the Ministry of Internal Affairs and Communications started research and development of quantum cryptography for satellite communications.

・On the other hand, these efforts are individual R&D initiatives undertaken by relevant ministries, agencies, and companies. These initiatives are not necessarily consistent. Therefore, the ”Quantum Technology Innovation Strategy” (January 2020) was compiled and published to promote quantum technology innovation by mobilizing the collective efforts of industry, academia, and government in Japan.

・Based on the Strategy, eight quantum technology R&D hubs (Quantum Computer R&D Hub (RIKEN), Quantum Device R&D Hub (National Institute of Advanced Industrial Science and Technology: AIST), Quantum Computer R&D Hub (University of Tokyo and Corporate Consortium), Quantum Software R&D Hub (Osaka University), Quantum Security Hub (National Institute of Information and Communications Technology: NICT), Quantum Material R&D Hub (National Institute for Materials Science: NIMS), Quantum Sensor Hub (Tokyo Institute of Technology), and Quantum Chemistry Hub (National Institutes for Quantum and Radiological Science and Technology：QST)) are currently conducting quantum technology

・In 2020, the Cabinet Office started research and development of quantum technologies, including quantum communications, under the “Moonshot Research and Development Program”, and the Ministry of Internal Affairs and Communications started research and development toward the creation of a global quantum cryptography network.

・NICT, as the ”Quantum Security Hub”, is conducting and promoting research and development of quantum cryptography and other key technologies for quantum networks.

(3) Quantum cryptography

[What kind of technology?]

・Quantum cryptography is a technology that uses the properties of quantum mechanics to make cryptographic communication unbreakable by any computer. It consists of two steps: quantum key distribution (QKD) and one-time pad encryption. QKD is a method of sharing symmetric cryptographic keys between two remote locations without revealing any information to a third party (eavesdropper) with any theoretical ability. In one-time pad encryption, a cryptographic key of the same size as the data (plaintext) is prepared, and a ciphertext is generated by the XOR of the plain text and the cryptographic key. The cryptographic key is discarded once by once, without reusing it. In this way, cryptographic communications with ”information-theoretic security” that cannot be deciphered in principle by any computer including quantum computers can be realized.

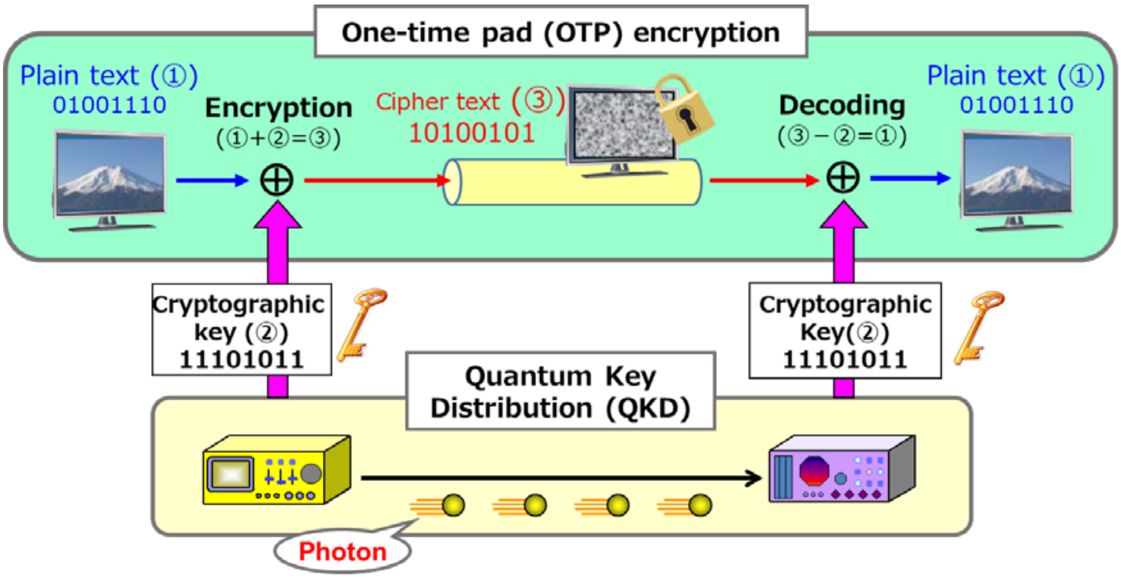


Figure 1 : Mechanism of Quantum Cryptography

[For what / why necessary?]

・ The cryptography which widely used today secures confidentiality in "computational security," which requires a huge amount of computing power to decrypt them. However, there is a potential threat that decryption will become easier in the future with the emergence of quantum computers and completely new computing technologies and mathematical algorithms. In particular, in the case of critical information that requires confidentiality for decades, a malicious third party may launch a so-called "harvest now, decrypt later" attack, in which encrypted data is eavesdropped and obtained for the time being, without having the technology to decrypt it, and the encrypted data is decrypted after establishing new computing technology in the future.

・On the other hand, quantum cryptography has information-theoretical security that cannot be decrypted in principle by any computer in the future. The only cryptographic technology that can achieve information-theoretical security is quantum cryptography at present. In this sense, quantum cryptography can achieve the strongest level of confidentiality among currently known cryptographic technologies. Quantum cryptography can be used to protect national secrets in such as national security, and to protect information that requires ultra-long-term confidentiality in fields such as medical, finance, infrastructure, and smart manufacturing.

[International trends]

・ Research and development and social demonstrations are progressing in countries such as Japan, Europe, the United States, China, and South Korea, and international standardization and full-scale practical application are starting.

[Requirements that may be required]

・It is necessary to establish a QKD network technology that allows a large number of QKD transmitters and receivers to be connected to the network and operated safely and efficiently.

・By sharing the encryption key at any two points (or multiple points) through the QKD network and using the key at the conventional network (the classical network), security services using the information-theoretically secure encryption key are realized.

(4) Quantum network

[What kind of technology?]

・A quantum network is the communication infrastructure for distributing quantum information (quantum bits used in quantum computers, quantum entanglement state with quantum correlation, etc.) over networks instead of classical digital information (0,1), and is utilized for various applications.

・Distribution of quantum information through a quantum network is expected to enable quantum cryptography over longer distances than currently possible, as well as a quantum network of optical clocks (atomic clocks that generate precise optical signals) that can be connected to each other to keep time with an accuracy that is impossible with conventional technology.

・Moreover, by connecting multiple small- and medium-scale quantum computers to a quantum network, it would be possible to build a large-scale quantum computer with high computing power (distributed quantum computing). Furthermore, by connecting a large-scale quantum computer at a remote location to a quantum network, it is expected to be possible to perform secret quantum computation without anyone knowing the contents of the computation.

[International trends]

・Basic research on quantum physics, which is an elemental technology on a quantum network, has been conducted around the world. In Europe and the United States, efforts to demonstrate the operation principle in the field has started since around 2020, and in Japan, studies have started to build a testbed on a quantum network.

[Requirements that may be required]

・To realize a quantum network, the following elemental technologies are required: quantum memory technology for storing and processing quantum information, quantum interface technology for connecting optical signals and quantum memory, and quantum relay technology for relaying and transmitting quantum information (especially quantum entanglement) without destroying it. All of these technologies are still in the basic research stage, and trial and error is still being conducted with various material materials and candidate relay methods.

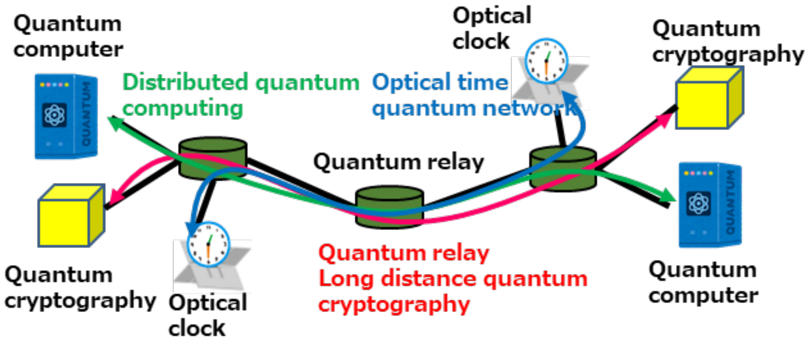


Figure 2 : quantum networks overview

(5) Quantum Internet

・The definitions of the ”Quantum Internet” are described as in the table below in the research strategies and projects on quantum technology in the United States and Europe.

・The “Quantum Internet” is a global quantum network to which quantum information equipment and devices such as quantum computers and quantum sensors are connected. Also, given that the current Internet is a network in which multiple networks are interconnected and digital information (bits) are distributed, the ”Quantum Internet” is a network in which multiple ”quantum” networks are interconnected and ”quantum information (qubits)” are distributed.”

・In the future, it is expected that the definition of ”Quantum Internet” will be clarified in the process of maturation of elemental technologies of ”Quantum Internet” through international discussions.

・When the Internet first appeared, no one imagined that the Internet would become indispensable infrastructure for socio-economic activities and people’s lives as it is today. At this point of time, it is not clear what kind of network the ”Quantum Internet” would be and how it would be used. However, it is expected that future applications and services that cannot be imagined at present will be provided on the ”Quantum Internet” in order to make people’s lives richer, safer and more secure.

	Document/ Organization	Definition example
The United States	”A STRATEGIC VISION FOR AMERICA'S QUANTUM NETWORKS”（2020.2), National Quantum Coordination Office, White House "A STRATEGIC VISION FOR AMERICA'S QUANTUM NETWORKS" (2020.2), National Quantum Coordination Office, White House	the quantum internet—a vast network of quantum computers and other quantum devices the quantum internet-a vast network of quantum computers and other quantum devices
	“Quantum Internet Blueprint Workshop” (2020.10), Department of Energy（DOE）"Quantum Internet Blueprint Workshop" (2020.10), Department of Energy (DOE)	The international research community perceives the construction of a first prototype global quantum network—the Quantum Internet—to be within reach over the next decade.　The international research community perceives the construction of a first prototype global quantum network-the Quantum Internet-to be within reach over the next decade.
Europe	Quantum Internet Alliance(QIA) Quantum Internet Alliance(QIA)	The long-term ambition of the European Quantum Internet Alliance is to build a Quantum Internet that enables quantum communication applications between any two points on Earth The long-term ambition of the European Quantum Internet Alliance is to build a Quantum Internet that enables quantum communication applications between any two points on Earth

	“Strategic Research Agenda on Quantum Technology” (2020.3), Quantum Flagship Project "Strategic Research Agenda on Quantum Technology"(2020.3), Quantum Flagship Project	“Quantum Internet”: quantum computers, simulators and sensors interconnected via quantum networks distributing information and quantum resources such as coherence and entanglement to secure our digital infrastructure. "Quantum Internet": quantum computers, simulators and sensors interconnected via quantum networks distributing information and quantum resources such as coherence and entanglement to secure our digital infrastructure.
Standard-ization body	IRTF （Internet Research Task Force）IRTF (Internet Research Task Force)	Quantum Internet - A network of Quantum Networks. The Quantum Internet will be merged into the Classical Internet to form a new Hybrid Internet. The Quantum Internet may either improve classical applications or may enable new quantum applications. Quantum Internet - A network of Quantum Networks. The Quantum Internet will be merged into the Classical Internet to form a new Hybrid Internet. The Quantum Internet may either improve classical applications or may enable new quantum applications.

Table 1 ： Examples of quantum internet definition

Chapter 2 : Image and Use Cases of a Society Realized by Quantum Networks

1. Image of society realized by quantum networks

(1) Overview

･The following is examples of the use cases that are expected to be realized by quantum networks in the future.

・In the 2020s, QKD networks are expected to enable secure exchange of critical information in the medical, manufacturing, and financial fields.

・In the 2030s and beyond, the spread of QKD networks is expected to enable the safe and secure distribution of information in a wider variety of fields. In addition, quantum networks connected with quantum computers and quantum sensors will begin to be deployed in society.

･In the 2040s, the "Quantum Internet", in which multiple quantum networks are globally connected to each other, will be established, and new applications and services will emerge that have never seen before. The ”Quantum Internet” is expected to become the foundation that supports people's affluent lives and socioeconomic activities.

	Use Case Example	Progress in quantum network technology	Quantum computing and sensing technologies
2020 s	● Medical care : Exchange of biological information, such as electronic medical records and genome information, that would have a lifetime impact if leaked ● Manufacturing : Exchange of information that has a significant impact on corporate activities due to leakage of trade secrets, know-how, important technologies, etc. ● Finance : Exchange of information on financial systems, transaction, etc.	· QKD (Kanto region → nationwide)	· NISQ Quantum Computer IBM[1] 2020 : 65 qubit 2021 : 127 qubit 2022 : 433 qubit 2023 : 1121 qubit
2030 s	● Administration / Diplomacy / Security : Exchange of personal information in administration, communication of confidential information in diplomacy, national security, etc. ● Life : Ultra-secure Internet at the home level through cryptography vending machines for mobile terminals to exchange of personal medical and financial information	· QKD (nationwide → global) · Satellite QKD/ physical layer encryption · Quantum networks	· NISQ Quantum Computer · Small-scale error tolerant quantum computers · Quantum sensor
2040 s	★ Chemicals, materials, drug discovery, etc. : Discovery of new materials and new drugs, etc. using quantum computers connected to quantum networks ▲Disaster prevention and disaster response: detection of weak gravity fluctuations by quantum sensors connected to quantum networks ●Resource development : High-precision image transmission of drilling robots on the Moon and Mars (Quantum coding beyond Shannon limitation)	· QKD (global scale) · Satellite quantum communication · Quantum networks (global scale)	· Error tolerant quantum computer · Distributed quantum computing · Quantum sensor

Example of use case ● : QKD, ★ : Quantum computer, ▲ : E quantum sensing

Table 2: Quantum Networks Use Cases (Overview)

2. Image of society and use cases realized by quantum key distribution (QKD) networks

(1) Information to be protected by the QKD network

·Security, diplomacy, defense, and personal genome information, all of which a significant impact if leaked, must be protected over a long period of time. When sending such information over a network, it is expected that QKD, which guarantees information-theoretical security, will be used.

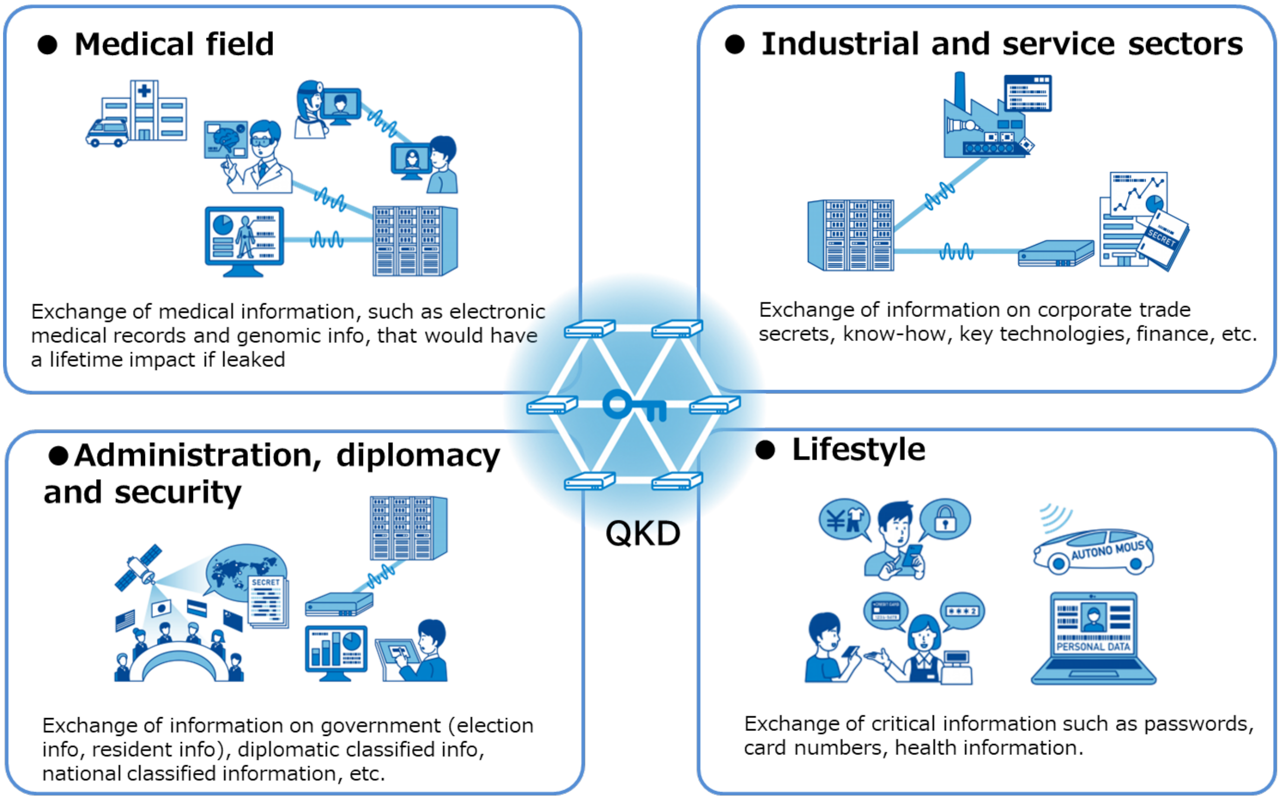
[1] https://www.ibm.com/blogs/think/jp-ja/ibm-quantum-roadmap/

Information holder	Examples of information to be protected
National/ local governments	・Diplomatic info, defense info, security info, geographical info. (infrastructure, underground space), family register / resident info, voting info, etc.
Organization (Enterprises, etc.)	・Customer lists, new business plans, price info, response manuals, etc. (sales info.) ・New technologies, manufacturing methods, know-how, design drawings, etc. (technical information) , etc.
Individual	・Health info, genome info, ideas, beliefs, preferences, personal identification numbers, credit card numbers, passwords, etc.

Table 3 ： Examples of information to be protected by QKD

(2) Image of society and use cases realized by QKD

・ Deployment of QKD will enable theoretically secure communications in medical, industry , services, government, diplomacy, , security, and daily life.



● Medical field

Exchange of medical information, such as electronic medical records and genomic info, that would have a lifetime impact if leaked

● Industrial and service sectors

Exchange of information on corporate trade secrets, know-how, key technologies, finance, etc.

●Administration, diplomacy and security

Exchange of information on government (election info, resident info), diplomatic classified info, national classified information, etc.

● Lifestyle

Exchange of critical information such as passwords, card numbers, health information.

Figure 3 : Examples of Use Cases Realized by QKD

(3) Examples of use cases in individual fields

①Medical and Financial Fields ~ Secure Data Distribution / Storage / Utilization with Quantum Secure Cloud ~

・It is an important task to store large amounts of information, which is one of the important management resources of a company, using encryption and other methods, and to decrypt them completely as necessary.

・At present, communication can be secured by current encryption technology. However, with the advancement of quantum computers, there is a risk that the encryption used for highly secure information communication for electronic payments and the exchange of personal information will be broken. Therefore, encryption technology that will never be broken is required.

[Technical outline]

・Quantum secure cloud technology is a cloud technology that enables secure distribution, storage, and utilization of data by integrating quantum cryptographic technology, secret sharing technology, and post-quantum cryptographic technology. QKD networks and secret sharing enable information-theoretically secure data storage and communication. The authentication infrastructure (post-quantum/public key authentication infrastructure) based on post-quantum cryptography, which require an enormous amount of computation to decipher, is used to authenticate users on the network and issue signatures to prevent tampering.

・The establishment of quantum secure cloud technology will not only ensure high security that cannot be tampered with or deciphered, but will also enable the collection, analysis, processing, and use of highly confidential data, such as personal and corporate information accumulated in the medical, new materials, manufacturing, and financial fields.

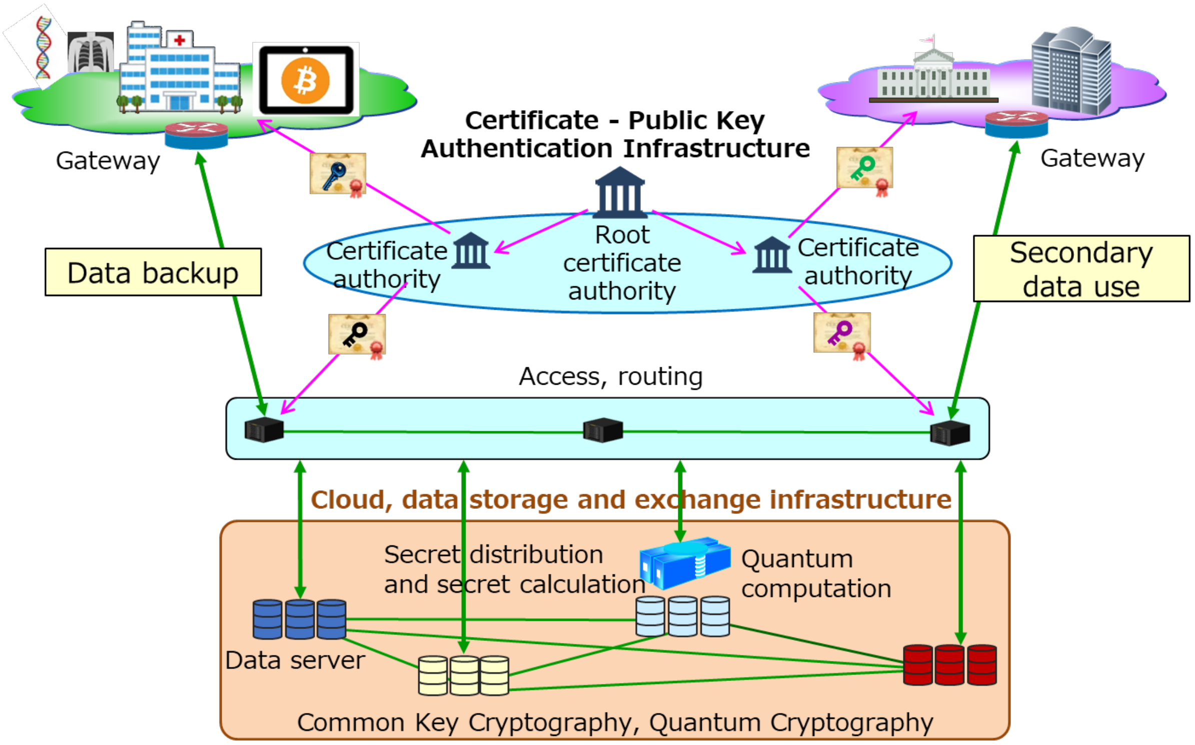

Certificate - Public Key
Authentication Infrastructure
Gateway
Gateway
Data backup
Certificate authority
Root certificate authority
Certificate authority
Secondary data use
Access, routing
Cloud, data storage and exchange infrastructure
Secret distribution and secret calculation
Quantum computation
Data server
Common Key Cryptography, Quantum Cryptography

Figure 4 : Mechanism of quantum secure cloud technology

②Administration, diplomacy and security ～Secure core network with satellite QKD～

［Background and necessity］

･QKD network needs to spread across Japan and across continents in order to securely exchange information related to national security and confidentiality, as well as personal information in local governments, across a wide area such as between cities and countries.

･However, QKD is vulnerable to signal attenuation in principle, which makes long distance transmission of quantum cryptography using optical fiber difficult. Therefore, satellite-based quantum cryptography communication networks in space, in which signal attenuation is lower than that of optical fibers, play an important role to realize a wide-area QKD network.

･In addition to the link between geostationary orbit satellites and the ground, the QKD backbone network based on satellite QKD enhances robustness and availability by utilizing multiple satellites (constellation satellites) in low and medium earth-orbit and cooperation with the terrestrial QKD network.

・In the future, it is expected to play a role as infrastructure for exploration and development by establishing quantum communication links with the Moon and Mars.

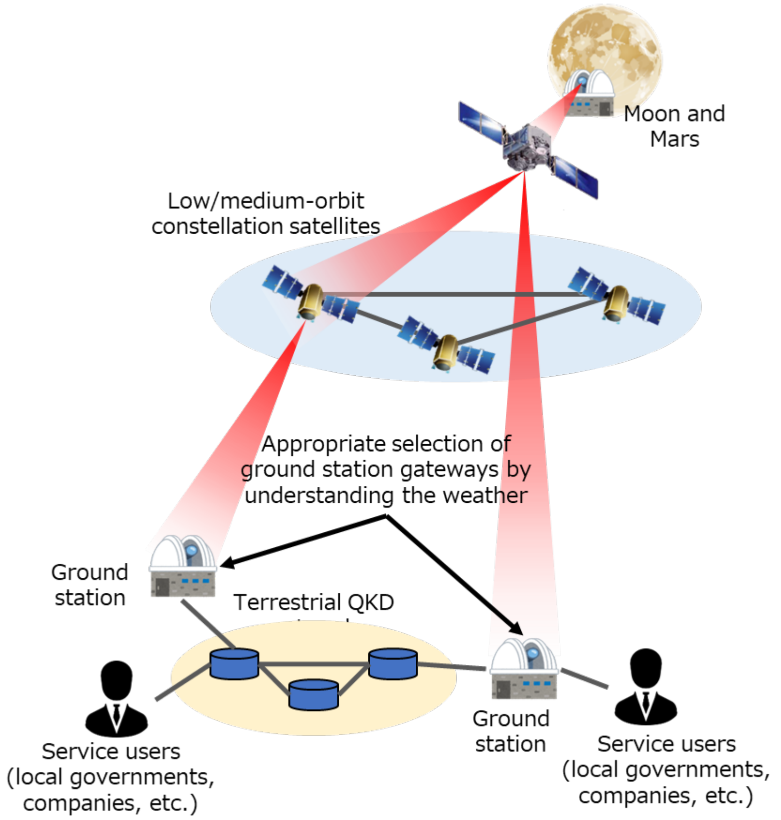

Moon and Mars
Low/medium-orbit constellation satellites
Appropriate selection of ground station gateways by understanding the weather
Ground station
Terrestrial QKD
Ground station
Service users (local governments, companies, etc.)
Service users (local governments, companies, etc.)

Figure 5 ： Secure backbone network with satellite QKD

③ Industry and service area ～Local secure network by optical space communication～

[Background and necessity]

・The trade secrets, know-how, and technical information that companies have accumulated over many years are important information in the industrial and service sectors. One of ways to protect this information from information leakage by industrial espionage is to use a local secure network using free space optical (FSO) communication, which can be built independently by companies on a scale of their premises, office buildings, and major branch offices.

[Technical outline]

・A secure network that can be built independently by companies is required to : (1) be able to be built independently of external organizations ; and (2) be able to be built at low cost. Among several QKD protocols, CV-QKD (Continuous Variable - Quantum Key Distribution), a system that is expected to be able to be built at low cost with the equipment and components used in current optical communications, can be implemented in optical space communications. By implementing this system in FSO communications, a secure network that satisfying the above requirements can be built without procuring and installing new optical fibers. In addition, by combining this system with secure communications (physical layer cryptographic communications) (see Chapter 4), which utilizes the unique characteristics of optical space communications, i. e., the spatial divergence of light is smaller than that of radio waves, making it difficult for third parties to eavesdrop, it is possible to build a network that can meet various user requirements.

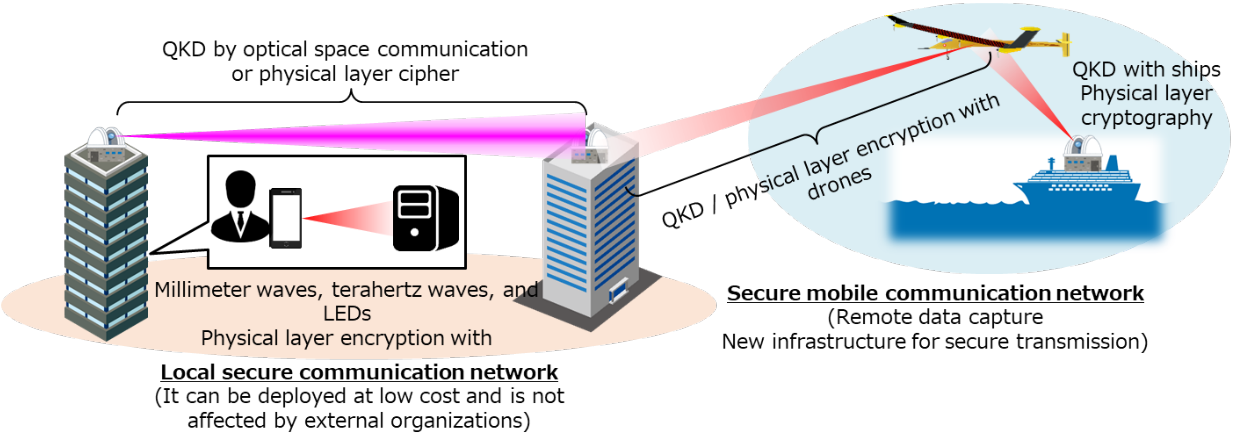

QKD by optical space communication
or physical layer cipher
QKD with ships
Physical layer
cryptography
QKD / physical layer encryption with
drones
Millimeter waves, terahertz waves, and
LEDs
Physical layer encryption with
Local secure communication network
(It can be deployed at low cost and is not
affected by external organizations)
Secure mobile communication network
(Remote data capture
New infrastructure for secure transmission)

Figure 6 ： Local Secure Network with QKD and Physical Layer Encryption

④ Daily life ～Highly secure infrastructure available to everyone～

[Background and necessity]

・ With the development of 5G technology, as services via mobile devices become more prevalent in people’s lives, personal security risks including leakage of important information in everyday life(e.g., passwords, credit card numbers, and health information), takeover of smart devices (e.g., network cameras, smart appliances, and smart speakers), will emerge. In order to ensure security at individual level, greater consideration is required to avoid differences in security level between individuals and organizations such as security providers.

・Therefore, we need a new security infrastructure that updates the security technology used in the current security infrastructure.

[Technical outline]

・In this infrastructure, key exchange and authentication on a conventional network (classical network) is carried out by cryptographic technology (post-quantum cryptography) that is difficult to break even by quantum computers. Communication between a mobile terminal and an access point is carried out by physical layer cryptography, which further enhances security of networks. Since these technologies can be implemented as algorithms on mobile terminals, individuals can use this infrastructure without being forced to bear a heavy burden.

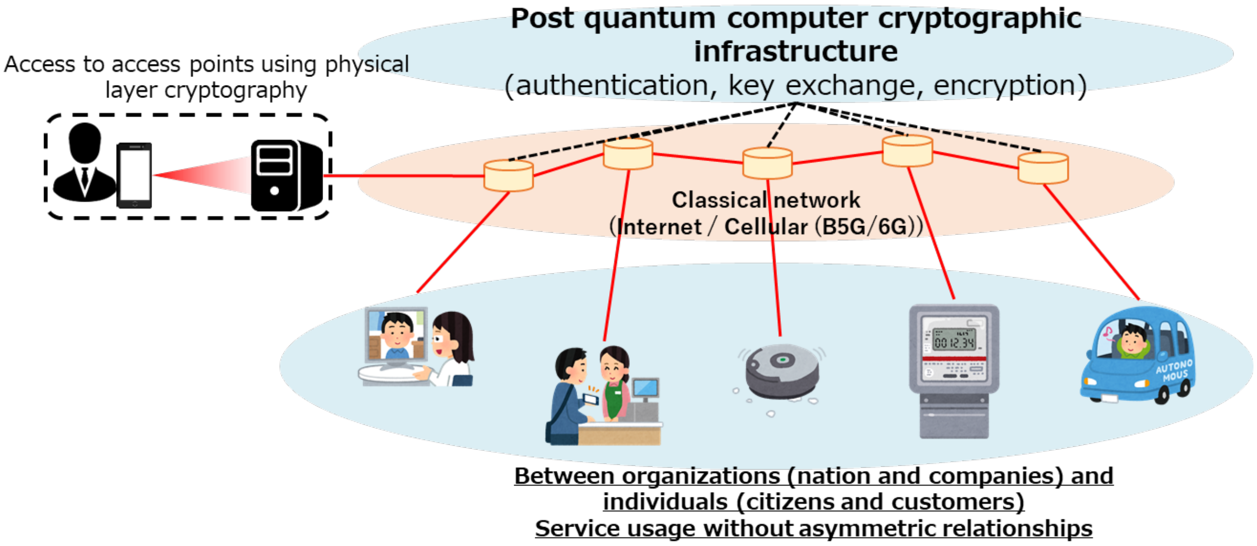

Post quantum computer cryptographic infrastructure
(authentication, key exchange, encryption)
Access to access points using physical layer cryptography
Classical network
(Internet / Cellular (B5G/6G))
Between organizations (nation and companies) and individuals (citizens and customers)
Service usage without asymmetric relationships

Figure 7 : New security infrastructure with post quantum cryptography infrastructure

3. Image of society and use cases realized by quantum networks

(1) Image of society and use cases

・It is expected that the realization of quantum networks (the Quantum Internet) will lead to the realization of safe, secure and convenient lifestyles and advanced socioeconomic activities.

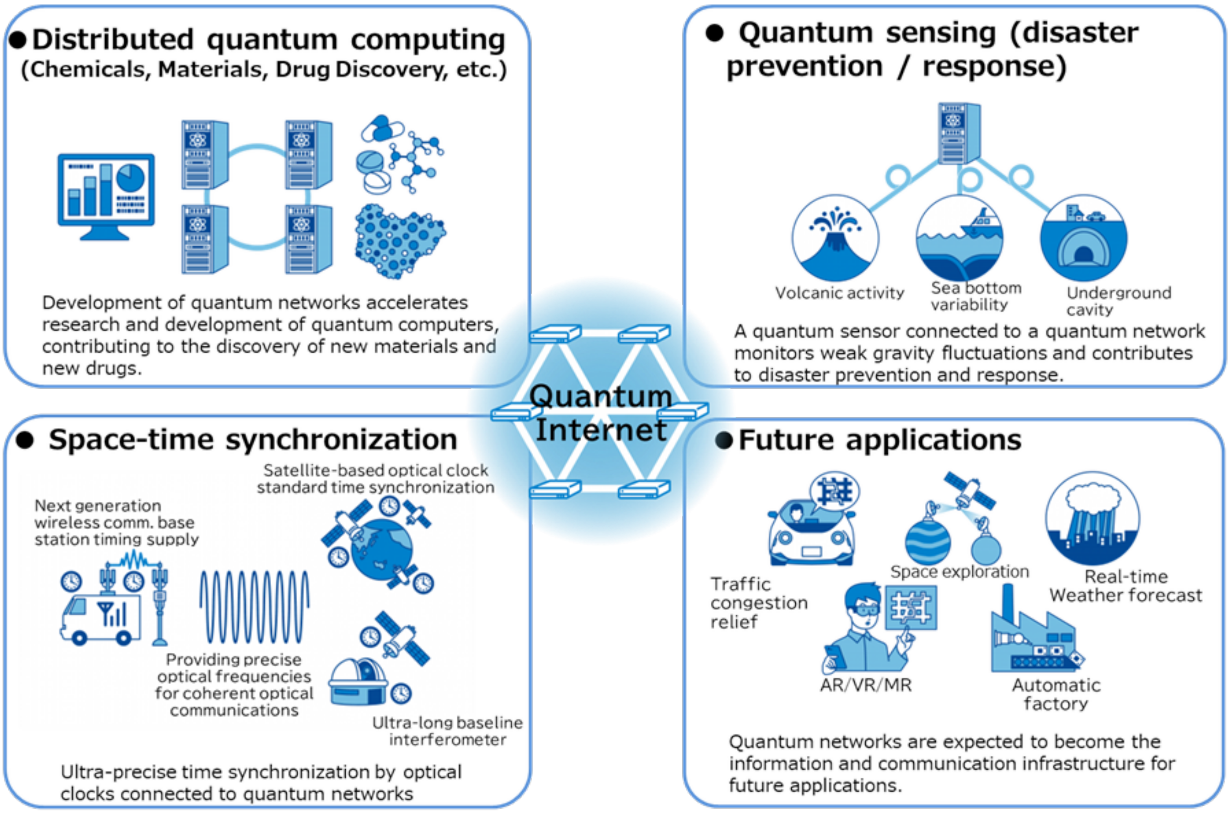

● Distributed quantum computing
(Chemicals, Materials, Drug Discovery, etc.)
Development of quantum networks accelerates research and development of quantum computers, contributing to the discovery of new materials and new drugs.
● Quantum sensing (disaster prevention / response)
Volcanic activity
Sea bottom variability
Underground cavity
A quantum sensor connected to a quantum network monitors weak gravity fluctuations and contributes to disaster prevention and response.
Quantum Internet
● Space-time synchronization
Satellite-based optical clock standard time synchronization
Next generation wireless comm. base station timing supply
Providing precise optical frequencies for coherent optical communications
Ultra-long baseline interferometer
Ultra-precise time synchronization by optical clocks connected to quantum networks
● Future applications
Traffic congestion relief
Space exploration
Real-time Weather forecast
AR/VR/MR
Automatic factory
Quantum networks are expected to become the information and communication infrastructure for future applications.

Figure 8 : Examples of image of society and use cases realized by quantum networks

(2) Examples of use cases in specific fields

①Quantum Sensing ～Disaster Prevention and Disaster Response ～

[Background and necessity]

・By connecting optical clocks (an example of the quantum sensors), which can provide high-precision timing and local gravity sensing, to a quantum network, and sending detected information on gravity field fluctuations such as earthquakes, volcanic eruptions, and landslides via the quantum network, it will be possible to issue disaster warnings earlier than before.

・In addition, the realization of highly accurate time and space synchronization is expected to lead to the emergence of next-generation communication systems and new time businesses.

[Technical outline]

・In order to transmit information such as gravitational field fluctuations detected by an optical clock using a quantum network, a technology called coherent link is a prerequisite. The coherent link is a technology to compare and synchronize the optical clocks by connecting their optical frequencies as light waves. The quantum network of optical clocks enables the fastest measurements of the optical frequencies of the clocks allowed by physics by adding it to the coherent link.

・In addition to the coherent link, other elemental technologies such as optical clocks capable of quantum gate operation, quantum interfaces with photons, and two-photon interference will be required.

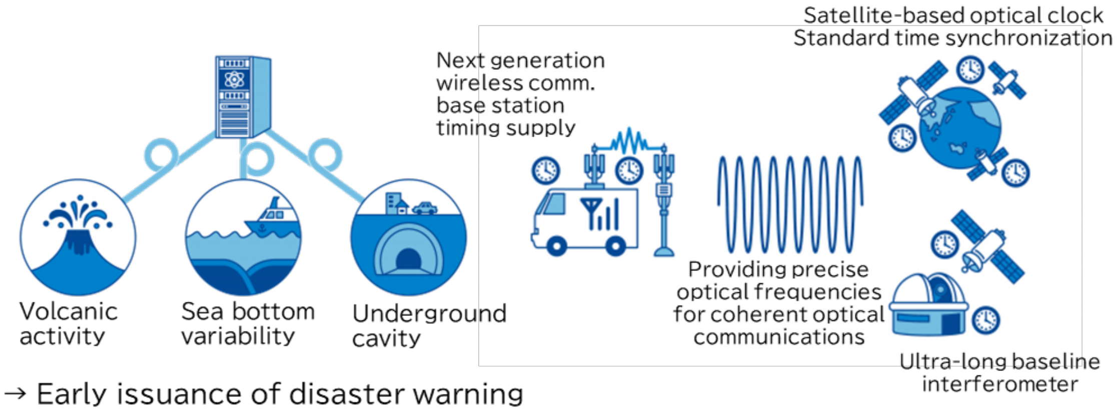


Figure 9 : Use cases of quantum networks for optical clocks

② Distributed Quantum Computing ～Chemistry, Materials, Drug Discovery, etc.～

[Background and necessity]

・Quantum computers will make it possible to simulate ultra-large scale molecular structures, which has been difficult with conventional supercomputers, and is expected to lead to drug discovery, materials with new functionalities, and new use cases for future social infrastructure.

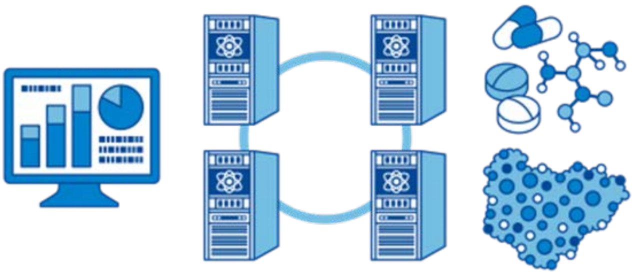
・Furthermore, by connecting quantum computers to a quantum network, it will be possible to accelerate the development of large-scale quantum computers.

・Since such large-scale quantum computation is expected to be provided by cloud services, a method to perform quantum computation while keeping the computation secret is required. Using a small-scale quantum computer connected to a large-scale quantum computer by a quantum network is expected to make such blind quantum computation possible.

[Technical outline]

・Quantum computing is a computational method that uses quantum bits (qubits) based on quantum physics instead of classical digital bits (0,1) to rapidly solve certain computational problems with computational resources that grow exponentially with the number of qubits (called "Hilbert space"). Distributed quantum computing is a method of extending quantum computing by connecting quantum computers in a quantum network.

・In order to connect quantum computers at the qubit level in a quantum network, a wide range of technologies are required. They include research and development of quantum repeaters and quantum network technologies for sharing quantum entangled states over optical fibers, as well as technologies for constructing small- and medium-scale quantum computers.



Development of quantum networks accelerates research and development of quantum computers, contributing to the discovery of new materials and new drugs.

Figure 10 ： Use cases for distributed quantum computer networks

Chapter 3 : Quantum Network Evolution

・Chapter 3 describes the evolution of quantum networks by the 2025s, 2030s, and 2040s.

・Quantum networks using QKD and quantum relays will be introduced step by step as the technology development and implementation. However, it does not mean that conventional networks such as the Internet and cell phone networks (classical networks) will be replaced by quantum networks, but rather that classical and quantum networks will coexist. The coexistence of classical networks and quantum networks will enable the realization of the various services described in the previous chapter. The following is an overview of the evolution of quantum networks.

1.Image around the year 2025

・The service operation of the quantum key distribution (QKD) network connecting the ground and satellite is expected to start, and that the secure communication service is expected to be provided. It is also assumed that the service using quantum computing and quantum sensing using classical networks is expected to be launched.

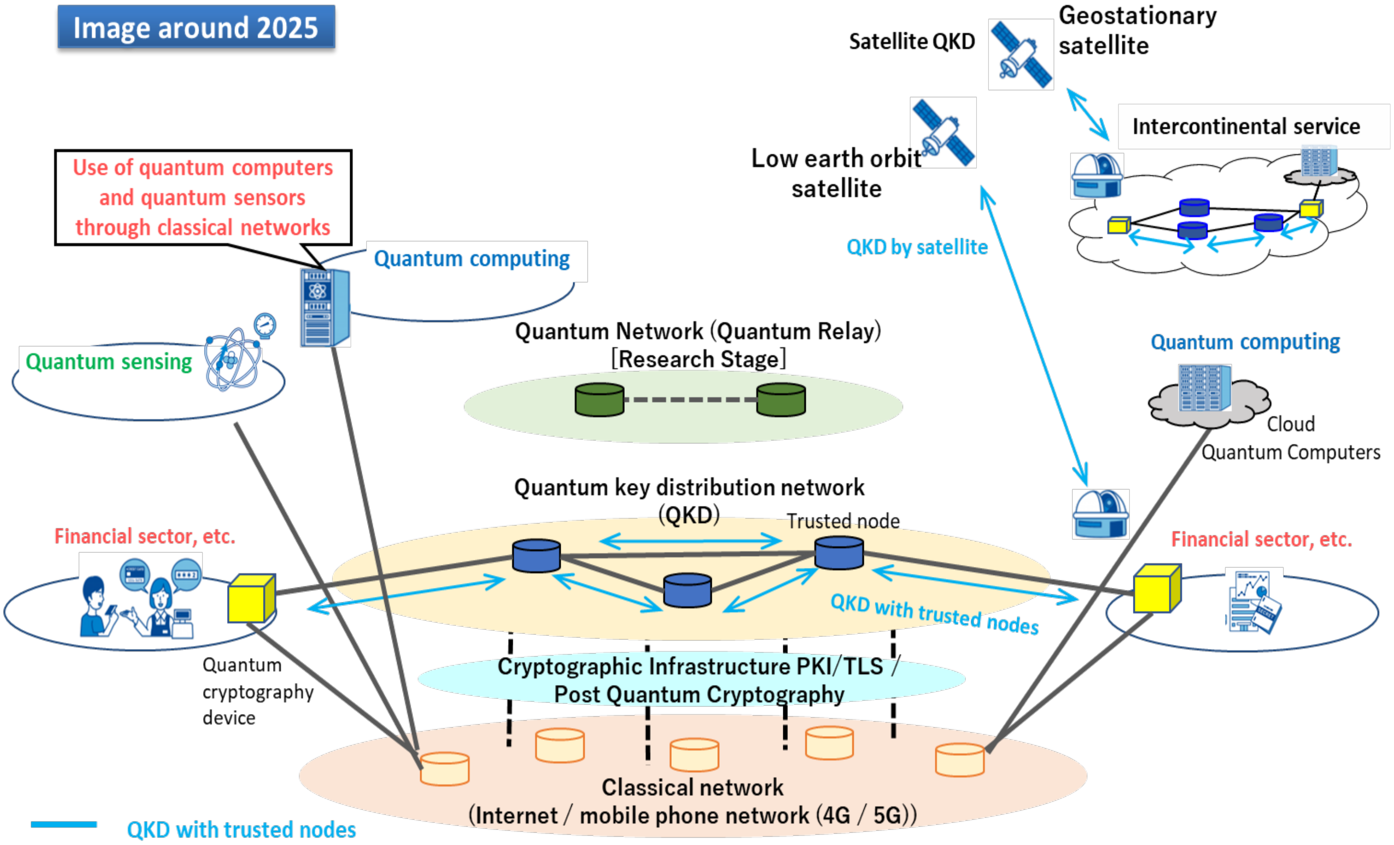


Figure 11: Evolution of quantum networks around 2025 [2]

2. Image around the year 2030

·The operation service of QKD networks connecting terrestrial and satellites secure communications services is expected to expand. In addition, services using quantum computing, quantum measurement and sensing over classical networks are expected to expand.

[2] PKI:Public Key Infrastructure, TLS: Transport Layer Security(A mechanism for ensuring a secure communication path for communication on the Internet)

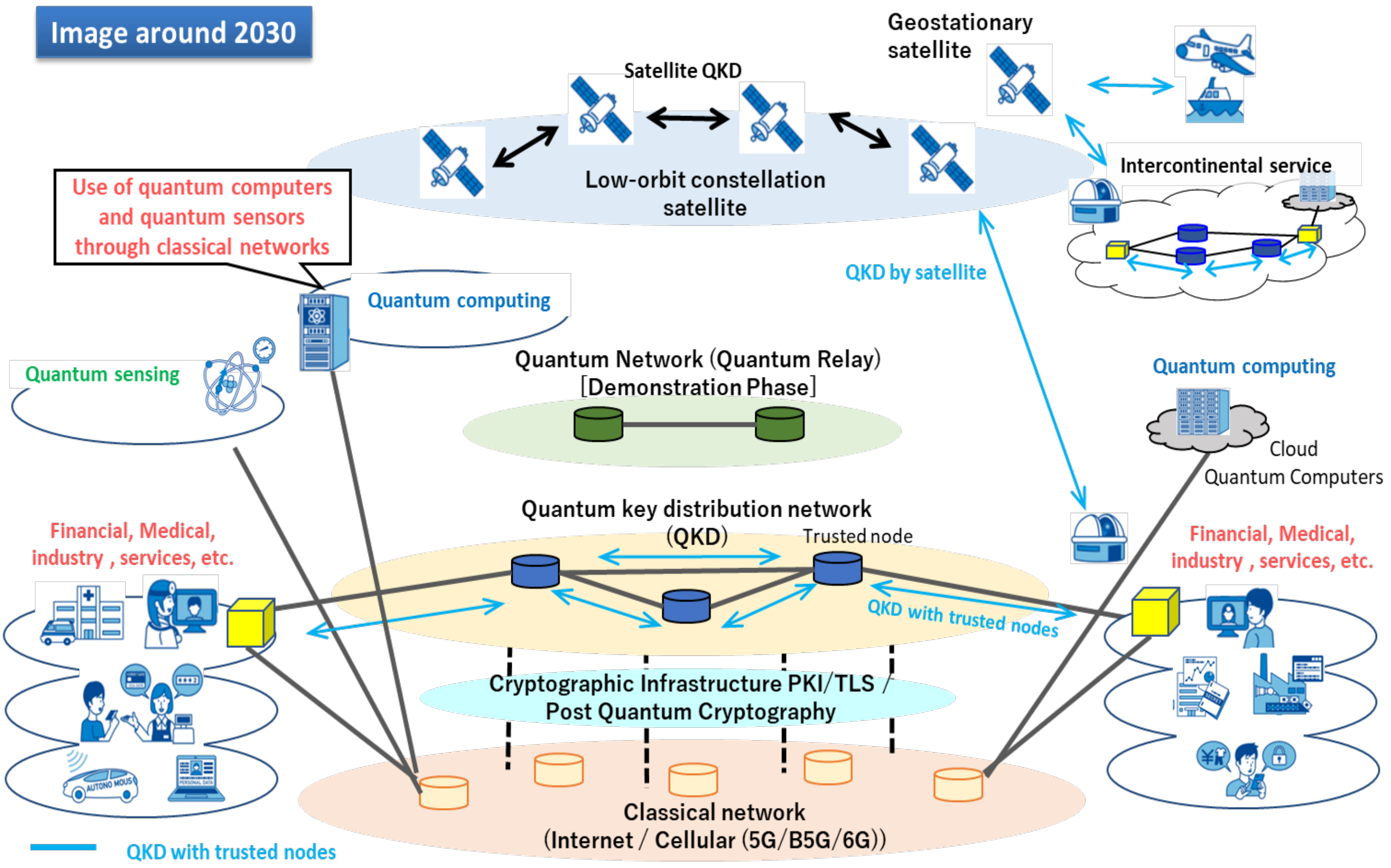


Image around 2030
Geostationary satellite
Satellite QKD
Low-orbit constellation satellite
Intercontinental service
Use of quantum computers and quantum sensors through classical networks
QKD by satellite
Quantum computing
Quantum sensing
Quantum Network (Quantum Relay) [Demonstration Phase]
Quantum computing
Cloud Quantum Computers
Quantum key distribution network (QKD)
Trusted node
Financial, Medical, industry , services, etc.
Financial, Medical, industry , services, etc.
QKD with trusted nodes
Cryptographic Infrastructure PKI/TLS / Post Quantum Cryptography
Classical network (Internet / Cellular (5G/B5G/6G))
QKD with trusted nodes

Figure 12 : Evolution of quantum networks around 2030

3. Image around the year 2040

・ It is assumed that a global quantum network of satellites and terrestrial networks will be established, and that a virtual quantum network service will be realized to accommodate a wide variety of quantum networks and protocols.

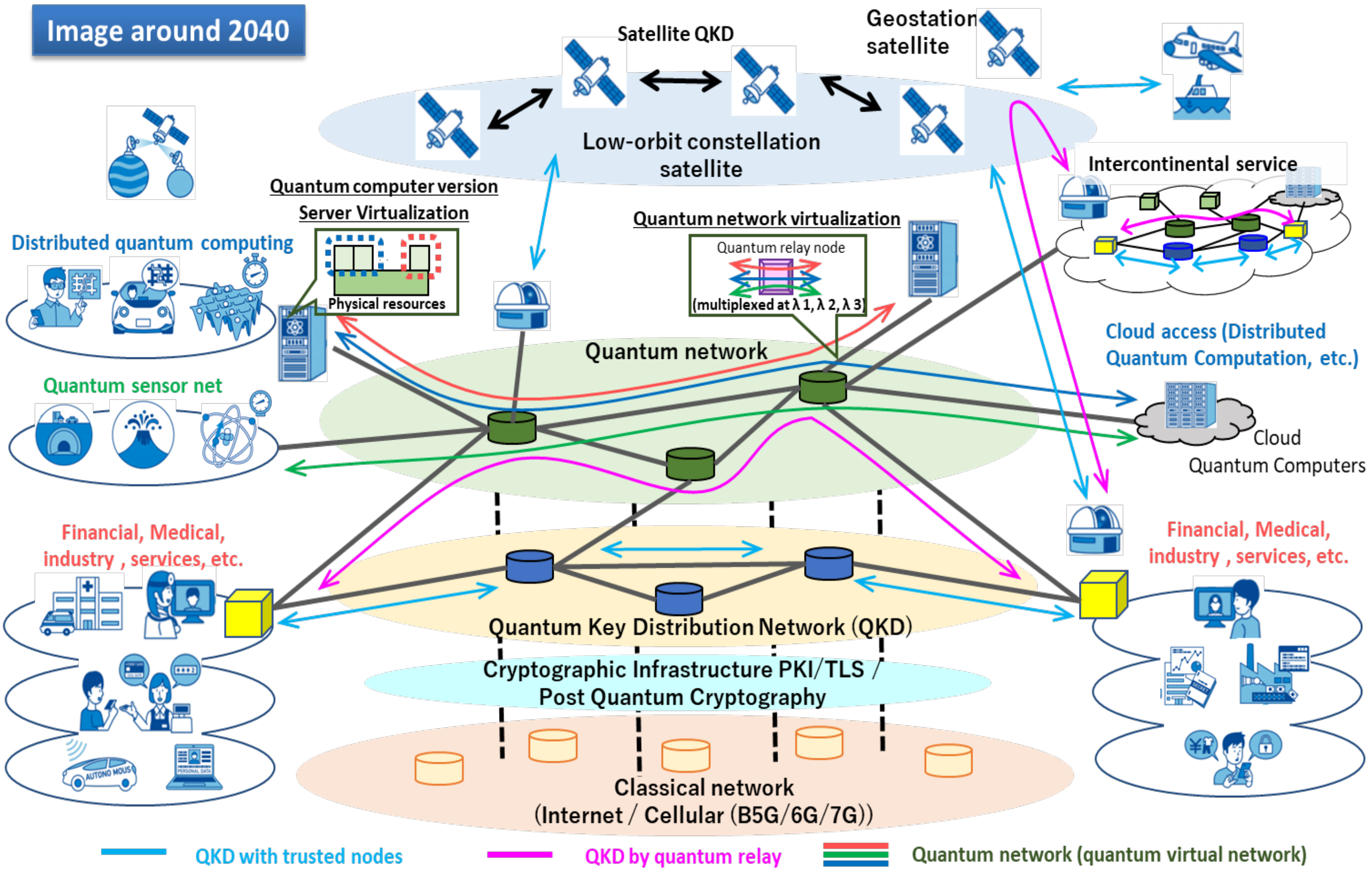


Image around 2040
Satellite QKD
Geostation satellite
Low-orbit constellation satellite
Intercontinental service
Quantum computer version Server Virtualization
Physical resources
Distributed quantum computing
Quantum network virtualization
Quantum relay node
(multiplexed at λ1, λ2, λ3)
Quantum network
Cloud access (Distributed Quantum Computation, etc.)
Cloud Quantum Computers
Quantum sensor net
Financial, Medical, industry , services, etc.
Financial, Medical, industry , services, etc.
Quantum Key Distribution Network (QKD)
Cryptographic Infrastructure PKI/TLS / Post Quantum Cryptography
Classical network (Internet / Cellular (B5G/6G/7G))
QKD with trusted nodes
QKD by quantum relay
Quantum network (quantum virtual network)

Figure 13: Evolution of quantum networks around 2040

・It is also assumed that infrastructure providers and quantum virtual network operators (VNOs) will construct virtual quantum networks and provide services in response to the requirements of application/content providers using quantum networks around 2040.

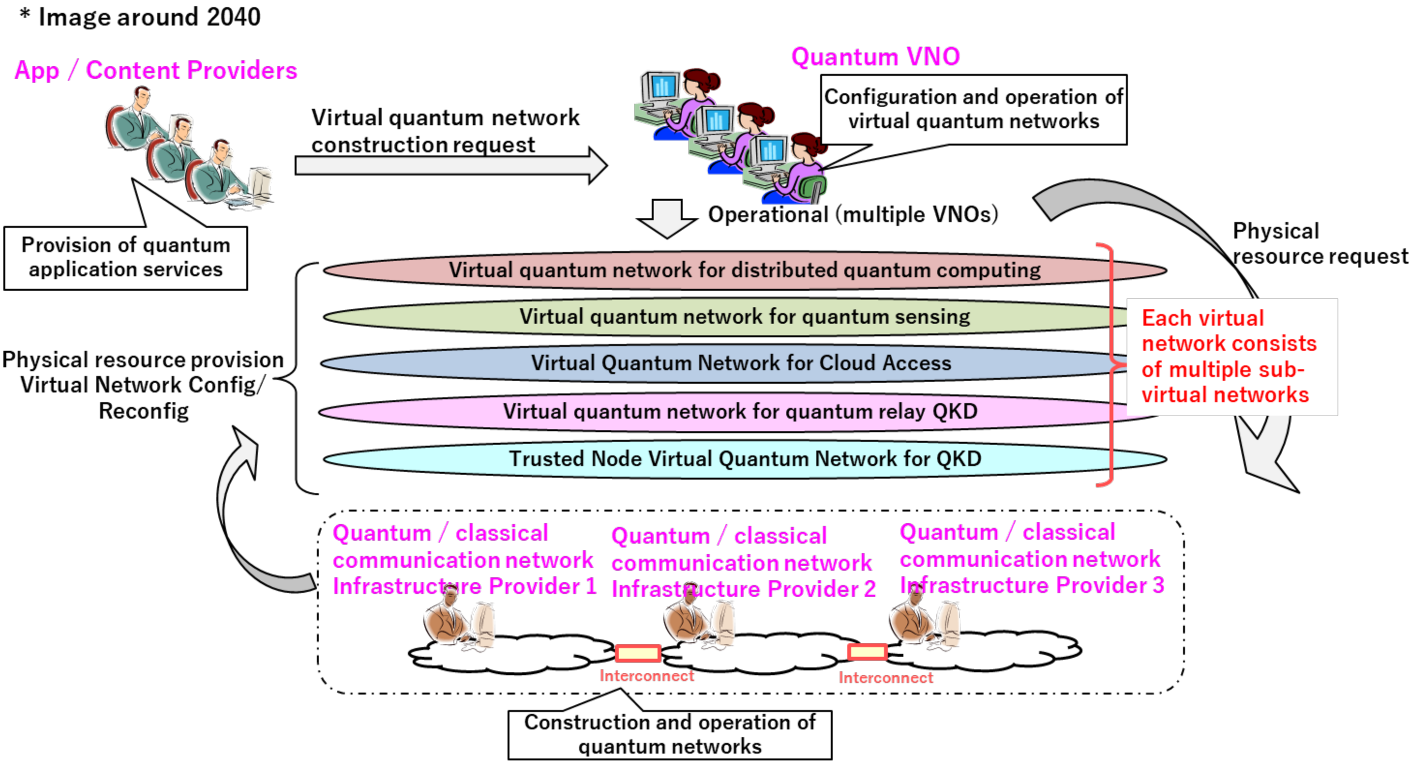

* Image around 2040
App / Content Providers
Provision of quantum application services
Virtual quantum network construction request
Quantum VNO
Configuration and operation of virtual quantum networks
Operational (multiple VNOs)
Physical resource request
Virtual quantum network for distributed quantum computing
Virtual quantum network for quantum sensing
Virtual Quantum Network for Cloud Access
Virtual quantum network for quantum relay QKD
Trusted Node Virtual Quantum Network for QKD
Each virtual network consists of multiple sub-virtual networks
Physical resource provision
Virtual Network Config/
Reconfig
Quantum / classical communication network Infrastructure Provider 1
Quantum / classical communication network Infrastructure Provider 2
Quantum / classical communication network Infrastructure Provider 3
Interconnect
Interconnect
Construction and operation of quantum networks

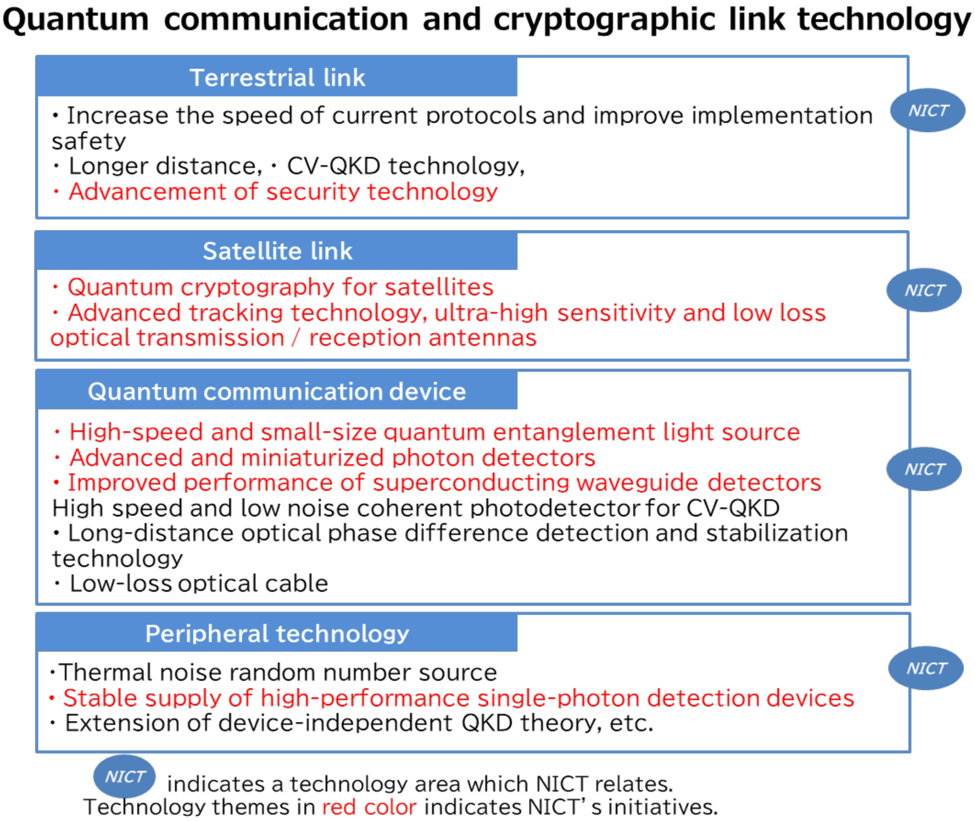
Figure 14 : Image of services in quantum networks around 2040

Chapter 4 : Element Technologies and Requirements

1. Overview of quantum network technology

(1) Overview of elemental technologies

・The chart below shows the elemental technologies of quantum networks in the "Quantum Technology Innovation Strategy" (January 2020). Of these, NICT is conducting R&D on technologies in red in the chart below.



Quantum communication and cryptographic link technology

Terrestrial link

・Increase the speed of current protocols and improve implementation safety
・Longer distance, ・CV-QKD technology,
・Advancement of security technology

NICT

Satellite link

・Quantum cryptography for satellites
・Advanced tracking technology, ultra-high sensitivity and low loss optical transmission / reception antennas

NICT

Quantum communication device

・High-speed and small-size quantum entanglement light source
・Advanced and miniaturized photon detectors
・Improved performance of superconducting waveguide detectors
High speed and low noise coherent photodetector for CV-QKD
・Long-distance optical phase difference detection and stabilization technology
・Low-loss optical cable

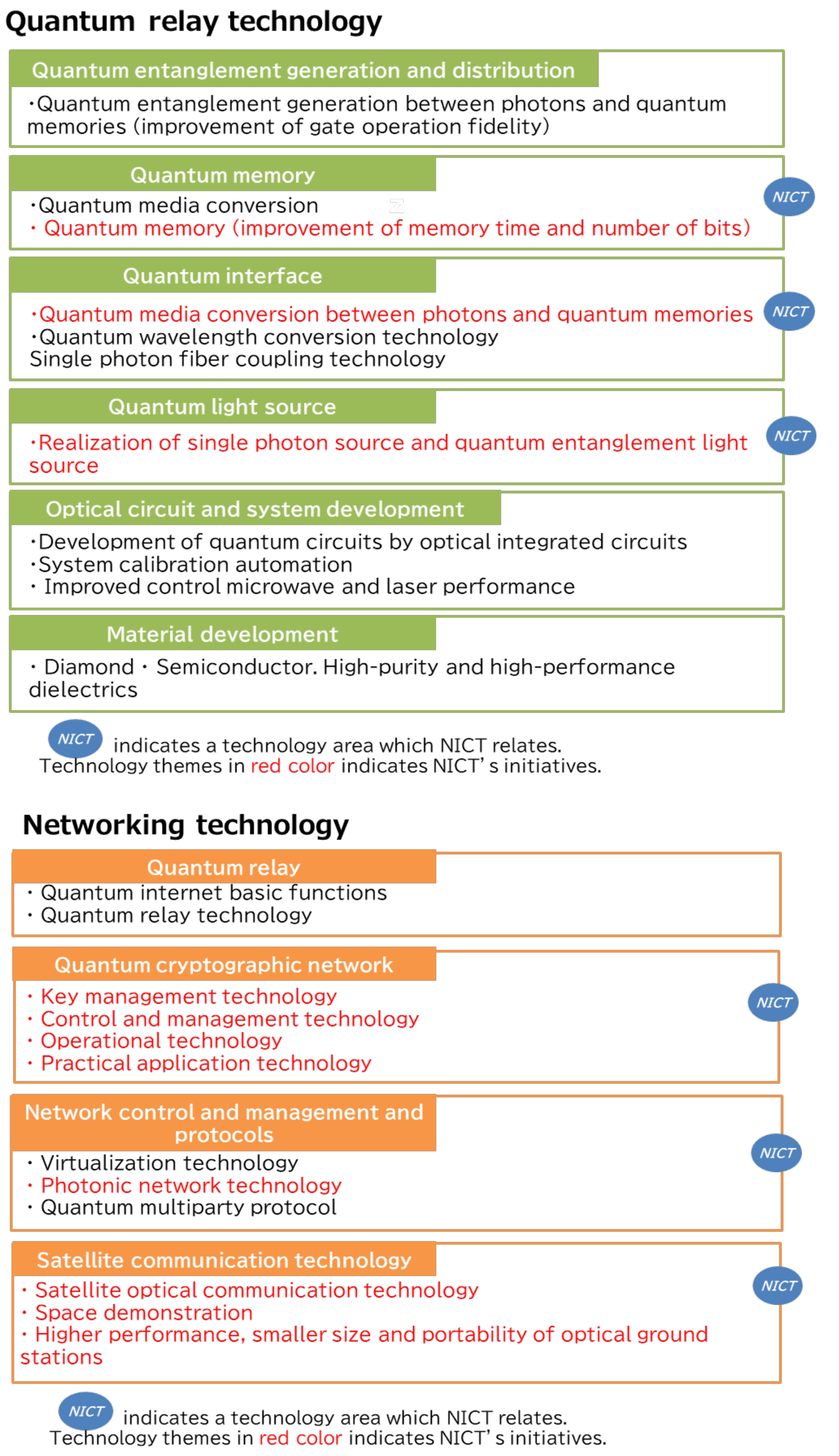
NICT

Peripheral technology

・Thermal noise random number source
・Stable supply of high-performance single-photon detection devices
・Extension of device-independent QKD theory, etc.

NICT

NICT indicates a technology area which NICT relates.
Technology themes in red color indicates NICT’s initiatives.



Quantum relay technology

Quantum entanglement generation and distribution

・Quantum entanglement generation between photons and quantum memories (improvement of gate operation fidelity)

Quantum memory

NICT

・Quantum media conversion
・ Quantum memory (improvement of memory time and number of bits)

Quantum interface

NICT

・Quantum media conversion between photons and quantum memories
・Quantum wavelength conversion technology
Single photon fiber coupling technology

Quantum light source

NICT

・Realization of single photon source and quantum entanglement light source

Optical circuit and system development

・Development of quantum circuits by optical integrated circuits
・System calibration automation
・ Improved control microwave and laser performance

Material development

・ Diamond・ Semiconductor. High-purity and high-performance dielectrics

NICT indicates a technology area which NICT relates.
Technology themes in red color indicates NICT' s initiatives.

Networking technology

Quantum relay

・ Quantum internet basic functions
・ Quantum relay technology

Quantum cryptographic network

NICT

・ Key management technology
・ Control and management technology
・ Operational technology
・ Practical application technology

Network control and management and protocols

NICT

・ Virtualization technology
・ Photonic network technology
・ Quantum multiparty protocol

Satellite communication technology

NICT

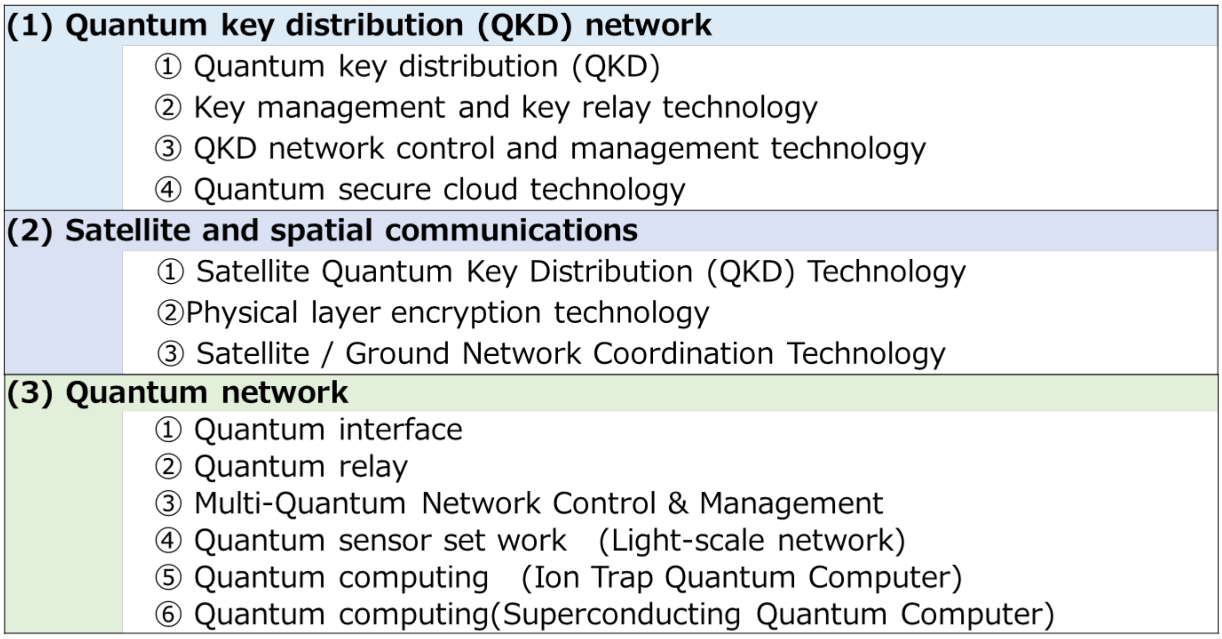
・ Satellite optical communication technology
・ Space demonstration
・ Higher performance, smaller size and portability of optical ground stations

NICT indicates a technology area which NICT relates.
Technology themes in red color indicates NICT' s initiatives.

Figure 15 : Overview of quantum network technologies

(2) Initiatives at NICT

・NICT is conducting R&D on quantum key distribution (QKD) networks, satellite and space communications, and quantum networks. The next section gives an overview of these elemental technologies and requirements.



(1) Quantum key distribution (QKD) network	
	① Quantum key distribution (QKD)
	② Key management and key relay technology
	③ QKD network control and management technology
	④ Quantum secure cloud technology
(2) Satellite and spatial communications	
	① Satellite Quantum Key Distribution (QKD) Technology
	②Physical layer encryption technology
	③ Satellite / Ground Network Coordination Technology
(3) Quantum network	
	① Quantum interface
	② Quantum relay
	③ Multi-Quantum Network Control & Management
	④ Quantum sensor set work (Light-scale network)
	⑤ Quantum computing (Ion Trap Quantum Computer)
	⑥ Quantum computing(Superconducting Quantum Computer)

Figure 16 : R&D on quantum network technologies at NICT

2. Elemental technologies and requirements

(1) Quantum key distribution (QKD) network

[Overview]

・A QKD network is a technology that makes it possible to share cryptographic keys to any two (or more) points in a network. The cryptographic keys shared in a QKD network are used for cryptographic communications in conventional networks (the Internet, mobile communication network, etc.) in which several application services are provided . In other words, by adding the QKD network to the conventional network, it is possible to provide a secure cryptographic key for a very long term. One of the applications of the QKD network is quantum secure cloud technology.

[Required Technologies]

・In addition to QKD equipment(QKD transmitters and receivers, called QKD modules), element technologies such as key management / key relay, QKD network control / management, are required. In addition, it is necessary to establish node security (trusted node).

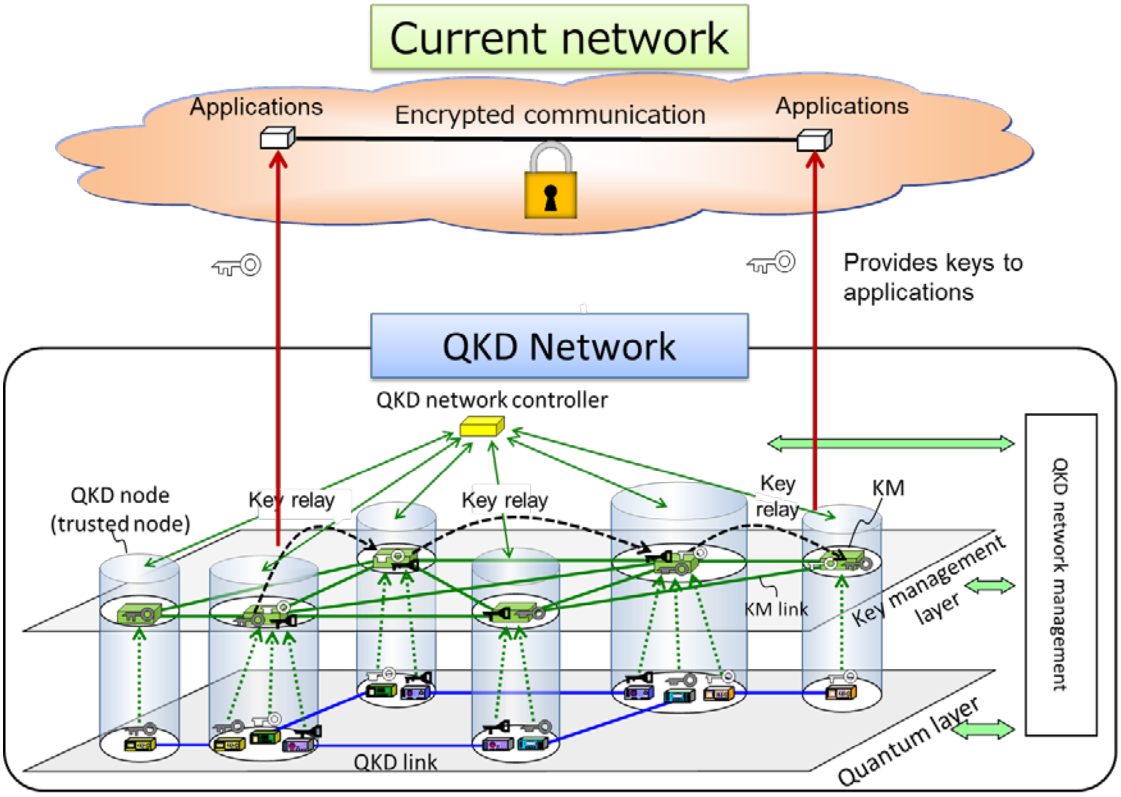


Figure 17 ： QKD network configuration

[International trends]

・Demonstration and test operations are underway in the United States, Europe, China, and South Korea, as well as Japan. The ”Tokyo QKD Network,” a testbed built in 2010 by Japanese companies, has the longest history of operation in the world.

As for QKD equipment, ID Quantique (Switzerland), Quantum CTek (China), Toshiba (Japan) and others have started commercialization and operation services, and NEC (Japan) is in the field test stage. In addition, a number of start-ups are developing QKD devices in various countries. QKD network services are also being commercialized by companies such as CAS Quantum Network (China) and Quantum Xchange (USA). Incumbent telecommunications companies such as BT (UK), Verizon (USA), and SK Telecom (Korea) are also entering the market.

[Reference] International standardization of QKD network technology

・NICT is actively promoting international standardization at the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) to promote the global spread of QKD network technology in cooperation with governments and companies.

・In October 2019, ITU-T published "Y. 3800 Overview on networks supporting quantum key distribution," the first international standard recommendation in the field of quantum cryptography, adopting the basic specifications of the Tokyo QKD network. Starting with this recommendation, ITU-T has published more than 10 recommendations. Japan is also leading the development of these recommendations.

・At ISO/IEC JTC1, NICT is actively participating in the development of standards for the safety assessment of QKD devices. Since QKD devices are security devices, it is necessary to develop safety and operational guidelines, as well as evaluation, testing, and certification framework to ensure that commercialized QKD devices are implemented and operated correctly from the viewpoint of safety, in order to properly distribute QKD devices in the market.

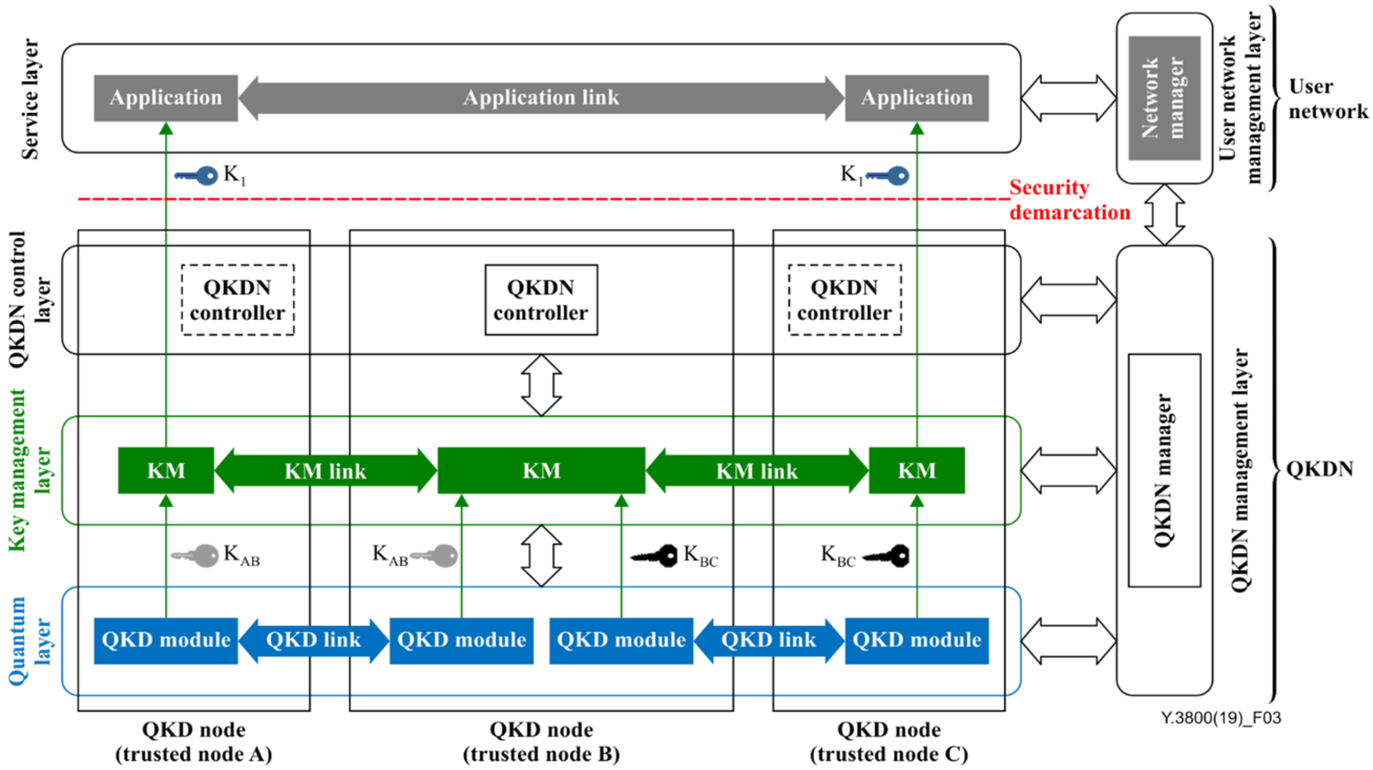


Figure 18 : Basic configuration of the QKD network specified in ITU-T Y. 3800 [3]

・The following is a description of the elemental technologies required for QKD network and its application, quantum secure cloud technology.

① Quantum key distribution (QKD)

[What kind of technology?]

・It is a technology to share encryption keys between two distant parties using photons, which are particles of light. Due to the uncertainty principle of quantum mechanism, any eavesdropping attack on photons can be certainly detected, By using cryptographic keys that is not eavesdropped, information-theoretically secure cryptographic keys can be generated. On the other hand, since photons are extremely weak signals and ordinary optical communication relay amplifiers destroy the quantum state of photons, the distance over which a pair of QKD transmitter / receiver can generate a key is currently limited to

[3] Abbreviations in Figure18 QKDN: QKD Network, KM: Key Manager

50-100 km at the most.

② Key management and key relay technology

[What kind of technology?]

・Key management is a technology that securely manages keys generated by QKD equipment and appropriately supplies them to applications. Key relay is a technology that securely transmits keys generated by QKD equipment to remote nodes through one-time pad encryption and a cryptographic key generated by another QKD equipment. By combining these technologies with node with guaranteed security (trusted node), long-distance key generation and QKD networking, which are impossible with a single QKD transmitter and receiver, are realized.

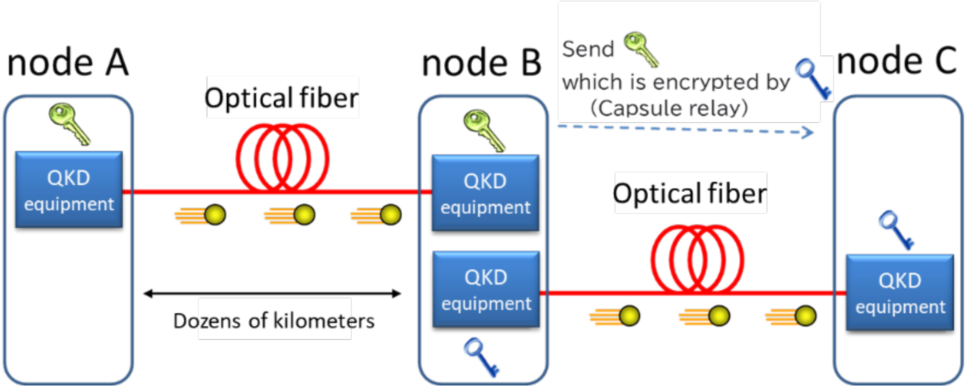


Figure 19 ： Quantum key relay mechanism

③ QKD network control and management technology

[What kind of technology?]

・The QKD network control technology is comprised of session control between sending and receiving hosts , access control, key relay routing and rerouting, policy control, network configuration control, etc. in the QKD network. The QKD network management technology appropriately manages the entire network by monitoring the status of network components and links in the QKD network. It is expected that conventional network control and management technologies, such as network virtualization/automation technology and information-centric networking technology, can be applied to the QKD network in various ways and thus, enable the network to efficiently deliver cryptographic keys with the required size and security level to users at any time.

④ Quantum secure cloud technology

[What kind of technology?]

•This technology enables data backup storage and computation processing that cannot be deciphered or tampered by any computer, by integrating quantum cryptography, secret sharing, post-quantum/public key authentication infrastructure, and secure computing. Multiple data servers are connected by secret lines using quantum cryptography to form a storage network, and secret sharing algorithms are implemented to the network to realize information-theoretically secure backup storage of the original data.

•In this way, the system provides both confidentiality, in which the original data cannot be recovered even if information is stolen from some of the data servers, and availability, in which the user can recover the original data by collecting distributed data from the remaining data servers even if some of the data servers are lost due to a disaster.

•In addition, it enables secure secondary use of the data, since it is possible to realize secure computing by processing the data in the meaningless distributed data.

• User authentication and data falsification prevention are performed using certificate with digital signatures issued from the post quantum -public key authentication infrastructure. The post quantum - public key authentication infrastructure is one of the next-generation cryptographic infrastructures that are expected to spread in the future and is based on computational security. For user authentication and prevention of data falsification on quantum secure clouds, the post quantum - public key authentication infrastructure is utilized because it is sufficient to secure security within the time required for processing.

• In this way, the entire system is configured by combining appropriate security technologies according to safety and convenience.

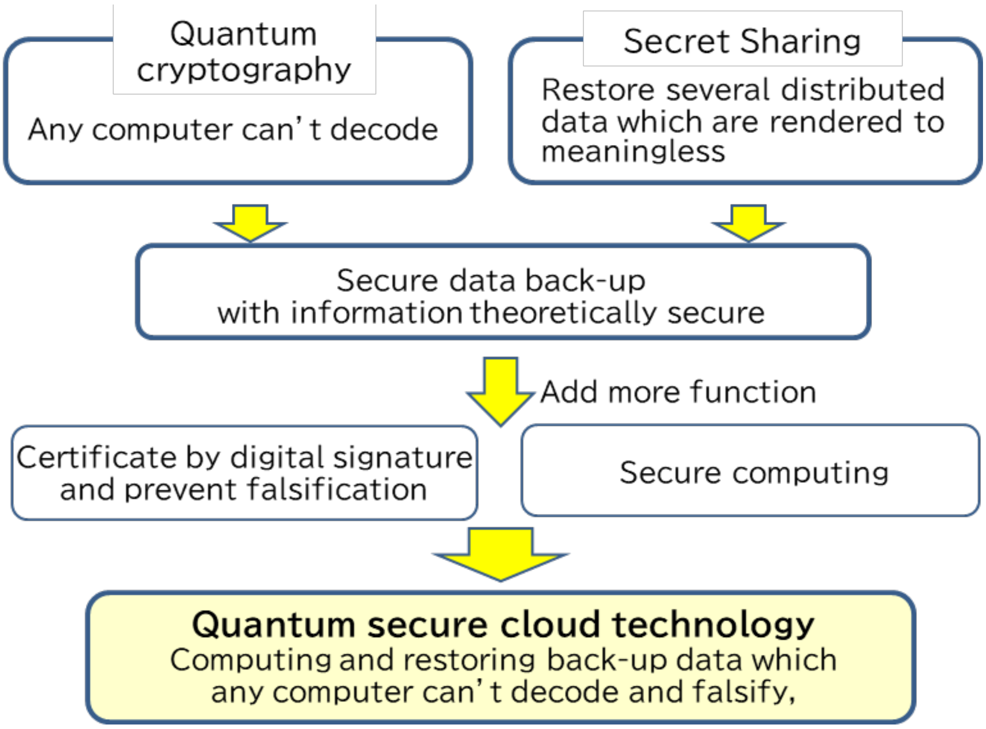

Quantum cryptography
Any computer can' t decode
Secret Sharing
Restore several distributed data which are rendered to meaningless
Secure data back-up with information theoretically secure
Add more function
Certificate by digital signature and prevent falsification
Secure computing
Quantum secure cloud technology
Computing and restoring back-up data which any computer can' t decode and falsify,

Figure 20 ： Quantum secure cloud technology

[For what / why necessary?]

・This technology is necessary to ensure ultra-long-term confidentiality of data. For example, medical information such as patient information and genetic data require ultra-long-term confidentiality. On the other hand, there is concern about data loss due to disasters, etc., if it is stored in only one hospital. It is also an urgent issue to safely back up data in remote locations. Quantum secure cloud can achieve both at the same time. (See ”Mechanism of quantum secure cloud technology” on p.20)

[International trends]

・This is a unique Japanese technology that is being demonstrated by NICT and companies.

[Requirements that may be required]

・It is necessary to appropriately integrate the QKD network and various modern security technologies (secret distribution, secret calculation, electronic signature, etc.) into a system.

(2) Satellite and spatial communications

① Satellite Quantum Key Distribution (QKD) Technology

[What kind of technology?]

・It is a technology to share information-theoretically secure cryptographic keys through quantum communication between ground and satellite or between satellites. (See "Secure backbone network with satellite QKD" on p.21.

[For what / why necessary?]

・In terrestrial QKD networks, the optical loss in optical fiber prevents QKD from being transmitted over long-distance, so a huge number of QKD devices and trusted nodes are required for globalization. On the other hand, the atmospheric layer surrounding the earth is about 10 km, and the optical loss in space is very small. Therefore, satellite-to-ground communication can greatly increase the transmission distance of QKD. Satellite QKD is an essential technology for the globalization of QKD networks.

[International trends]

・NICT has demonstrated quantum communication between a 50-kg small satellite and a ground station, which is the basis of the QKD[4]. Meanwhile, China has succeeded in the QKD experiment[5] between a low-earth orbit satellite and the ground. The momentum for accelerating satellite QKD research is growing among governments, universities, and venture companies around the world.

[Requirements that may be required]

・In addition to the development of a new QKD protocol optimized for satellite communications, it will be necessary to develop pointing acquisition and tracking technology as well as adaptive optics technology to stabilize the satellite-to-ground link, and

[4] H. Takenaka, et al., Nat. Photonics, (2017)

[5] S. -K. Liao, et al., Nature (2017)

high-speed and high-sensitivity single-photon detector technology to detect photons.

②Physical layer encryption technology

[What kind of technology?]

・Unlike QKD, which is ”secure against any physically allowable eavesdropping attack,” physical-layer cryptography is a technology for information-theoretically secure cryptographic key establishment in situations where restrictions can be placed on eavesdroppers' attack models, such as ”eavesdroppers eavesdrop from outside the sight of the sender or receiver.” (See ”Secure core network with satellite QKD” on p21, ”Local secure network with QKD and physical layer encryption” on p.22, and ”New security infrastructure with post quantum cryptography infrastructure ” on p.23)

[For what / why necessary?]

・This technology is used as a complementary technology to QKD in communication systems such as satellite-to-ground and mobile communications, where the current QKD does not provide sufficient performance or is difficult to implement.

[International trends]

・NICT is conducting physical layer cryptography research in free-space optical communications[6], and companies and universities dealing with QKD have applied for patents on similar concepts[7].

[Requirements that may be required]

・In order to apply physical layer cryptography to satellite-to-ground communication, it is necessary to develop protocols, technologies for establishing links such as pointing, acquisition and tracking systems, and high-speed and high-sensitivity single-photon detector technologies similar to satellite QKD technology.

[6] H. Endo, et al., Opt. Express, (2018), H. Endo, et al., OSA Continuum., (2020)

[7] M. Legre and B. Huttner, EP 3337063 A1, (2016)., E. J. A. Ling, et al., WO 2019/139544 A1, (2019). M. Legre and B. Huttner, EP 3337063 A1, (2016)., E. J. A. Ling, et al., WO 2019/139544 A1, (2019).

On the other hand, in order to apply physical layer cryptography to mobile communications, it is necessary to develop protocols suitable for high-frequency bands (millimeter waves, terahertz waves, and LEDs).

③ Satellite-terrestrial network coordination technology (adaptive routing technology)

[What kind of technology?]

・This technology is used for continuously providing secure communication services by selecting the optimum route and transmission protocol (QKD/physical layer encryption, etc.) for the entire satellite/terrestrial network, taking into consideration user requirements such as the required level of security and natural conditions such as weather. (See "Secure backbone Network with Satellite QKD" on p.21)

[For what / why necessary?]

・ For example, since satellite QKD / physical layer cryptography cannot be provided in cloudy weather, it is necessary to select a ground station in a sunny area. In order to provide secure service without fatal delay, the terrestrial network route must also be appropriately changed according to this ground station selection.

[International trends]

・The change of ground stations based on weather conditions in satellite optical communications is called site diversity, and NICT has been conducting R&D on this subject[8].

[Requirements that may be required]

・ Technologies are required to collect information on communication channels such as weather information and share it with satellite nodes and ground nodes. In addition, technologies are required to enable the miniaturization, portability, and installation on ships of ground stations in order to establish links with satellites at various locations on the

[8] K. Suzuki, ICSO2014, or OBSOC

ground.

(3) Quantum network

① Quantum interface

[What kind of technology?]

・It is a technology to transmit quantum information between different quantum physical systems without changing the quantum information. It is also called quantum media conversion.

[For what / why necessary?]

・It is needed to realize quantum connections via photons between quantum systems of matter that constitute spatially separated nodes.

[International trends]

・It has been reported that a fluorescent photon was generated from a quantum system of matter and converted into a communication wavelength band photon[9,10]. It has also been reported that a quantum connection between two spatially separated quantum systems of matter was formed via photons[11].

[Requirements that may be required]

・A quantum entanglement manipulation technique is required to generate quantum correlations between the matter quantum system and the emitted photons. High performance photon detectors are needed to measure the interference between the two photons generated at the sender and receiver with high efficiency. A quantum memory is needed to hold the quantum state until the photons propagate, the interference measurement, and manipulation into a quantum system of matter are performed.

[9] Phys. Rev. Lett. **120** 203601 (2018).

[10] Nat. comm. **9** 1998 (2018). npj Quant. Inf. **5** 72 (2019).

[11] Phys. Rev. Lett. 119 010402 (2017), Nature 578 240 (2020). Nature 526 682 (2015).

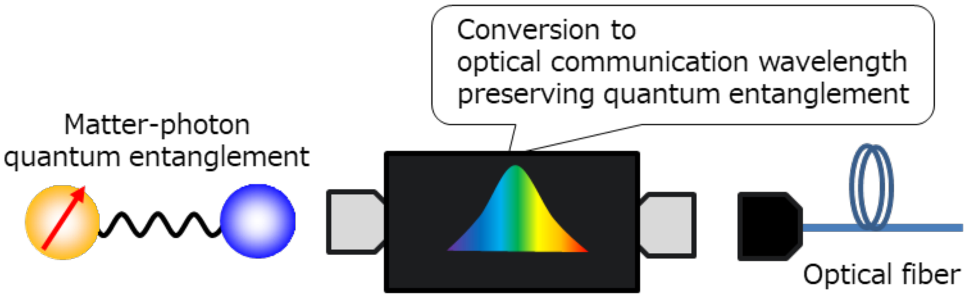

Conversion to
optical communication wavelength
preserving quantum entanglement
Matter-photon
quantum entanglement
Optical fiber

Figure 21 ： Role of the quantum interface

② Quantum repeater

[What kind of technology?]

・It is a technology that enables quantum information transmission over long distances by placing multiple quantum-connected nodes at relay points.

[For what / why necessary?]

・In principle, quantum states cannot be replicated, so signal attenuation due to loss in the communication channel cannot be recovered by amplification. Therefore, quantum repeater is necessary to extend the distance of quantum connections. It is also applicable to extend the distance of QKD.

[International trends]

・In Japan and overseas, research and development of standard methods consisting of quantum entanglement swapping, quantum entanglement purification, and quantum memory is underway. Improving the performance of quantum memory is considered to be the key to realization[12]. In addition, an all-optical quantum repeater protocol that does not use quantum memory has been proposed in Japan [13], and demonstration experiments are underway[14].

[12] Nature Photonics, 10, 381(2016)

[13] Nature Communications 6, p. 6787(2015)

[14] Nature Communications 10,378(2019)、Nature Photonics 13, 644 (2019)

[Requirements that may be required]

・In addition to quantum entanglement control techniques such as quantum entanglement swapping and quantum entanglement purification, a quantum memory is required to maintain the quantum state until the end of the series of operations. In the all-optical quantum repeater protocol, quantum memory is not required. High-performance photon detectors are required to observe photon interference in quantum entanglement operations with high efficiency.

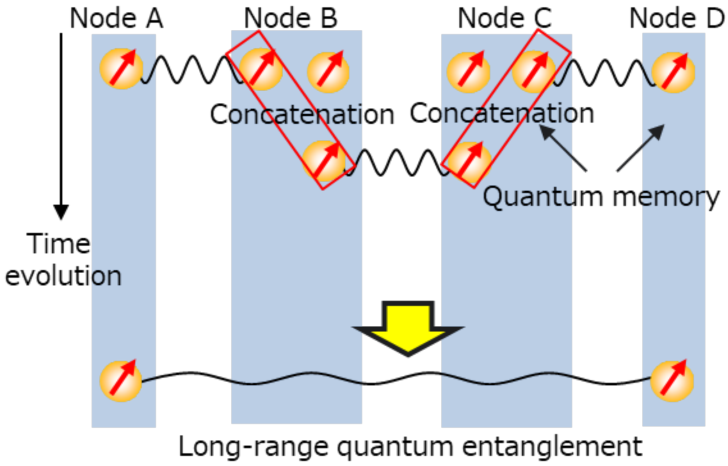


Figure 22 ： Quantum repeater mechanism

③ Multi-kind Quantum Network Control and Management

[What kind of technology?]

・This technology enables the stable and inexpensive provision of a wide variety of virtual quantum networks (including quantum computer virtualization) that satisfy the requirements / demands of various future applications, including QKD networks and quantum relay networks, on the same physical network.

[For what / why necessary?]

・It is necessary to satisfy various application requirements / demands (cryptographic key size in QKD, communication performance, stability of quantum applications, etc.) while reducing costs by saving physical devices managed by network operators.

[International trends]

・The ITU-T SG13 currently discusses software-defined network control (SDN control) and virtualization for QKD networks[15]. On the other hand, the IRTF currently discusses quantum internet (quantum relay network)[16] . In addition, several projects related to quantum networks have already been launched in Europe and the United States. In the United States, for example, the National Quantum Coordination Office launched by White House Office of Science and Technology Policy (OSTP) has published a report on the National Strategy of Quantum Information Science[17]. In Europe, the Delft University of Technology in the Netherlands has published a report on future quantum networks, including the quantum internet[18].

[Requirements that may be required]

・In order to construct virtual quantum networks that satisfy the requirements and demands of various applications, and to respond to changes in conditions such as network traffic fluctuations and fault detection, it is important to achieve agility and effectiveness in route selection, rerouting, resource allocation, and so on. It will enable the networks to enhance the stability of applications.

・Moreover, we can expect that it is effective to apply policy control (e.g.: SDN) and in-network computing technologies (e.g.: information-centric networking and network coding[19]) which have been actively researched and developed in classical networks.

・In addition, we will require advanced security technologies to ensure the safety and security of control and management mechanisms and also require integration of terrestrial- and

[15] ITU-T SG13 Y.QKDN-SDNC (June 2020)

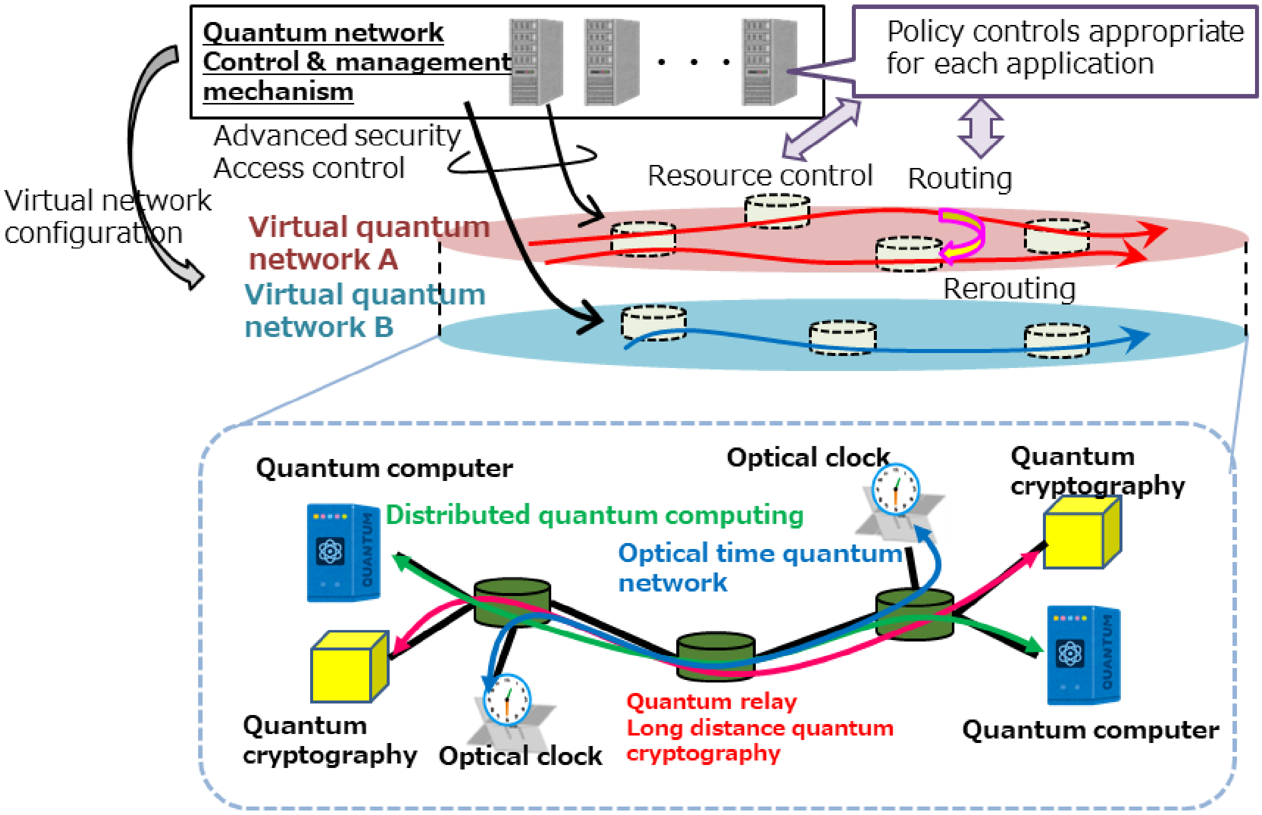
[16] ITRF QIRG-ID: “Applications and Use Cases for the Quantum Internet”(draft-irtf-qirg-quantum-internet-use-cases-04) (January 2021)

[17] “Quantum Frontiers: Report on Community Input to the Nation’s Strategy for Quantum Information Science, “ The White House National Quantum Coordination Office (October 2020)

[18] “Creating the Quantum Future – QuTech Annual Report 2019,” Delft Univ. of Tech. (March 2019)

[19] K. Matsuzono, et. al., “Low Latency Low Loss Streaming using In-Network Coding and Caching”, Proc. IEEE Infocom (May 2017).

satellite-based network technologies to realize global virtual quantum networks in the future.


Quantum network Control & management mechanism
・・・
Policy controls appropriate for each application
Advanced security
Access control
Resource control
Routing
Virtual network configuration
Virtual quantum network A
Virtual quantum network B
Rerouting
Quantum computer
Optical clock
Quantum cryptography
Distributed quantum computing
Optical time quantum network
Quantum cryptography
Optical clock
Quantum relay
Long distance quantum cryptography
Quantum computer

＊ Including quantum cryptography by trusted node QKD.
Satellite and terrestrial system are integrated

Figure 23 ： Quantum network mechanism

④ Quantum sensor network (Quantum network of optical clocks as an example))

[What kind of technology?]

・Devices that use quantum effects to measure physical quantities are called quantum sensors. Atomic clocks that use the optical frequencies are called optical clocks, and they are also used as quantum sensors to measure gravity. Coherent links that connect optical clocks with optical fibers or free space enable distribution of space-time information and gravity crowdsensing without deploying quantum network technology. In a quantum network of optical clocks, an extension of the link supported by quantum connections, the measurement speed can be reduced to the limit allowed by physical laws.

[For what / why is it necessary?]

・It is required for the realization of high-precision timing distribution for next-generation communications, phase synchronization for coherent optical communications, and ultra-long baseline interferometry. As a gravity sensor, it is considered to be effective for monitoring underground cavities, magma reservoirs, and seafloor fluctuations.

[International trends]

・Construction of a coherent link with a total length of more than 2000 km is in progress in Europe[20]. In Japan, RIKEN, the University of Tokyo, NICT, and other organizations are conducting R&D on a coherent link. A link with a total length of 240 km has been reported[21]. The quantum network of optical clocks has been proposed only, and no actual implementation has been reported so far[22].

[Requirements that will be required]

・A coherent link that faithfully transmits the frequency accuracy of the optical clock is required. To plug in quantum connectivity, a quantum interface between atoms or ions and photons is required. When the fiber length between optical clocks exceeds 100 km, quantum repeaters are required.

[20] https://www.clonets.eu/clonets-consortium.html

[21] Optics Express,28,9186 (2020)

[22] Nature Physics, 10, 583 (2014)

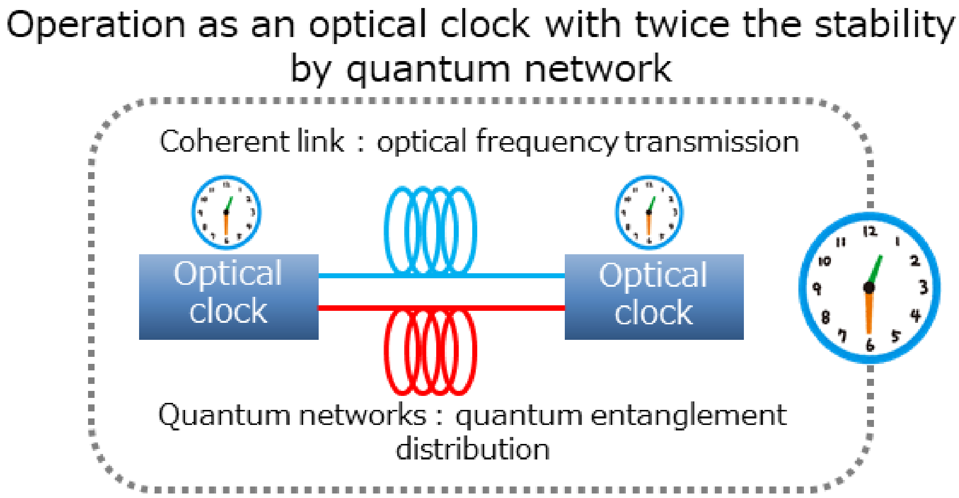

Operation as an optical clock with twice the stability by quantum network
Coherent link : optical frequency transmission
Optical clock
Optical clock
Quantum networks : quantum entanglement distribution

Figure 24 ： Quantum network of optical clocks

⑤ Quantum computing (Ion trap quantum computer)
[What kind of technology?]

・An ion trap quantum computer consist of atomic ions laser-cooled in an ion trap as qubits. All the qubits are connected via the phonons of the oscillating motion caused by the trap electric field as a quantum bus. An ion trap quantum computer with a quantum interface between ions and photons is called an optically connected ion trap quantum computer.

[For what / why it is necessary?]

・A ion-trap quantum computer with a single ion trap is considered to be limited to about 50 qubits due to fundamental and technical limitations. Large-scale quantum computation is expected to be possible by connecting multiple ion-trap quantum computers via photons.

[International trends]

・In the U.S. and Europe, ion-trap quantum computers with up to 32 qubits without optical connectivity have been realized, and cloud quantum computing services have been launched[23]. An ion-trap quantum computer with optical connectivity has not yet been

[23] https://ionq.com/, https://www.aqt.eu/

realized, and research and development are underway in the United States and Europe with the goal of achieving 50 qubits[24]. In Japan, research and development has begun under the Moonshot Research and Development program[25].

[Requirements that will be required]

・We need a highly functional ion trap with a quantum interface with photons that can perform quantum computation with about 10 qubits. Quantum wavelength conversion technology is required to convert the wavelength of the photons generated by the ion trap into the optical communication wavelength for connecting to an optical switch. Two-photon interference technology and high-performance photon detectors are required to perform optical connection operations.

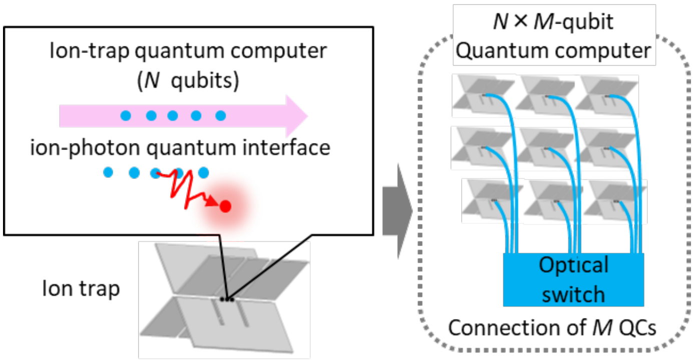


Figure 25 ： Optically connected ion trap quantum computer

⑥ Quantum computing (superconducting quantum computer)

[What kind of technology?]

・ Superconducting electric circuits cooled to cryogenic temperatures behave quantum mechanically, and they are called superconducting quantum circuits. Superconducting quantum circuits have a high degree of freedom in their design, and can be made into qubits, resonant circuits, waveguides, coupled circuits, and so on. A superconducting quantum computer is a system

[24] https://www.aqtion.eu/

[25] https://www.jst.go.jp/moonshot/program/goal6/index.html

consisting of a large number of qubits capable of qubit gate operation and state measurement.

[For what / why necessary?]

・Quantum computers are assumed to be much more powerful than present computers in solving certain class of problems by deploying quantum mechanical resources to computation. Superconducting quantum computers are considered to be one of the most promising candidates for quantum computers because of their high degree of freedom in design and integration.

[International trends]

・In 2019, Google demonstrated quantum supremacy in a sample containing 53 qubits[26]. Thus, research and development of NISQ (Noisy Intermediate-Scale Quantum computer) [27] , a superconducting quantum computer consisting of several tens of qubits without error correction, is actively conducted. In Japan, the Q-LEAP Flagship project[28] and the Moonshot Research and Development program[29] are conducting research and development.

[Requirements that may be required]

・Research and development of qubits with long coherence time is necessary. In addition, microwave transmission technology with low reflection and loss, high-precision microwave pulse generation technology, high-sensitivity microwave measurement technology, and high-speed signal processing technology are required for high-speed and high-precision qubit gate operation, qubit measurement, and quantum feedback. Furthermore, it is necessary to increase the cooling power of dilution refrigerators and to improve the reproducibility of superconducting quantum circuit fabrication technology.

[26] https://www.nature.com/articles/s41586-019-1666-5

[27] https://doi.org/10.22331/q-2018-08-06-79

[28] https://www.jst.go.jp/stpp/q-leap/

[29] https://www.jst.go.jp/moonshot/program/goal6/index.html

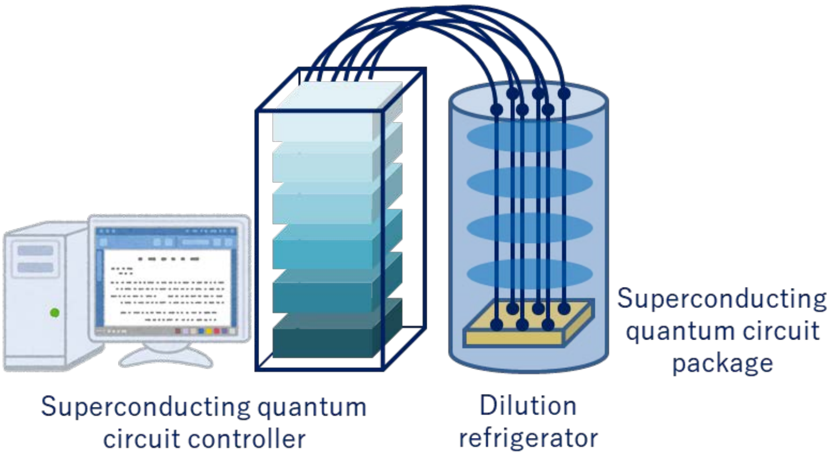
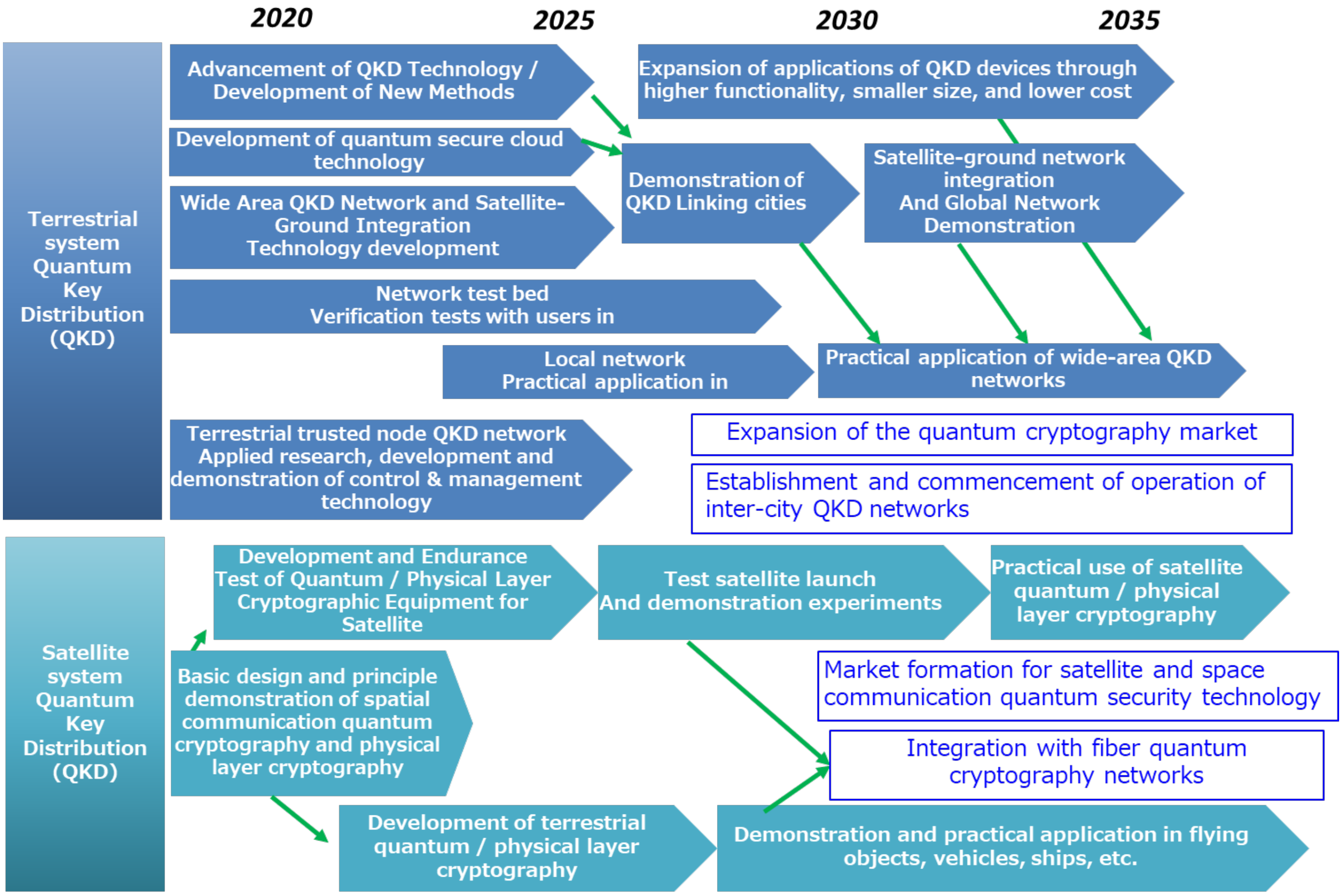

Superconducting quantum circuit package
Superconducting quantum circuit controller
Dilution refrigerator

Figure 26 ： Superconducting quantum computer

Chapter 5 : R&D Roadmap

・For the elemental technologies in Chapter 4, we have compiled a roadmap for the period from 2020 to 2035. The roadmap for research and development of terrestrial and satellite quantum key distribution (QKD) networks is as follows.



2020 2025 2030 2035

Terrestrial system Quantum Key Distribution (QKD)

Advancement of QKD Technology / Development of New Methods

Development of quantum secure cloud technology

Wide Area QKD Network and Satellite-Ground Integration Technology development

Network test bed Verification tests with users in

Local network Practical application in

Terrestrial trusted node QKD network Applied research, development and demonstration of control & management technology

Expansion of applications of QKD devices through higher functionality, smaller size, and lower cost

Demonstration of QKD Linking cities

Satellite-ground network integration And Global Network Demonstration

Practical application of wide-area QKD networks

Expansion of the quantum cryptography market

Establishment and commencement of operation of inter-city QKD networks

Satellite system Quantum Key Distribution (QKD)

Development and Endurance Test of Quantum / Physical Layer Cryptographic Equipment for Satellite

Test satellite launch And demonstration experiments

Practical use of satellite quantum / physical layer cryptography

Basic design and principle demonstration of spatial communication quantum cryptography and physical layer cryptography

Market formation for satellite and space communication quantum security technology

Integration with fiber quantum cryptography networks

Development of terrestrial quantum / physical layer cryptography

Demonstration and practical application in flying objects, vehicles, ships, etc.

Figure 27 ： R&D Roadmap for QKD network

・The roadmap for research and development of quantum networks is as follows.

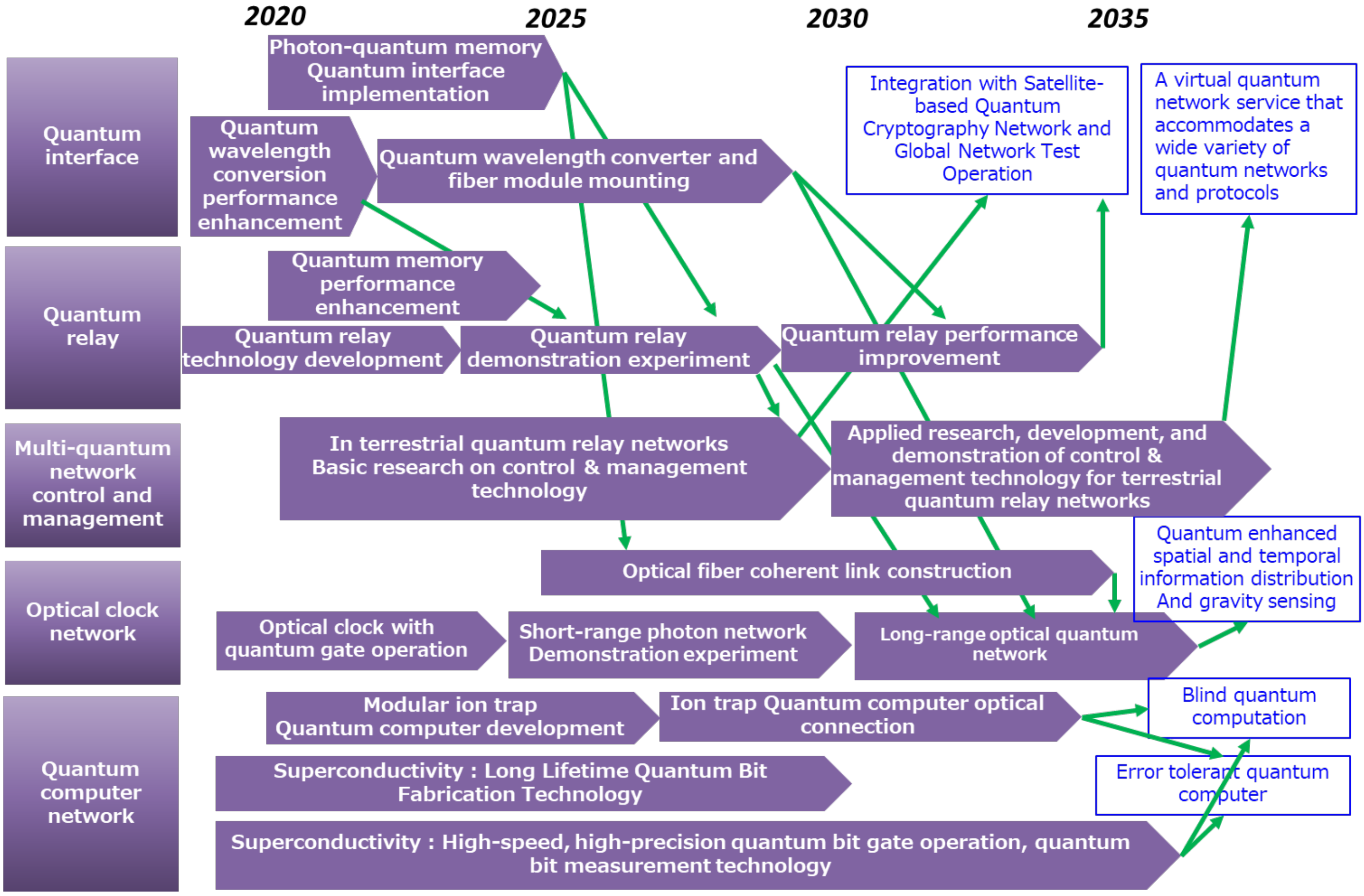

2020
2025
2030
2035
Quantum interface
Quantum relay
Multi-quantum network control and management
Optical clock network
Quantum computer network
Photon-quantum memory Quantum interface implementation
Quantum wavelength conversion performance enhancement
Quantum wavelength converter and fiber module mounting
Quantum memory performance enhancement
Quantum relay technology development
Quantum relay demonstration experiment
Quantum relay performance improvement
Integration with Satellite-based Quantum Cryptography Network and Global Network Test Operation
A virtual quantum network service that accommodates a wide variety of quantum networks and protocols
In terrestrial quantum relay networks Basic research on control & management technology
Applied research, development, and demonstration of control & management technology for terrestrial quantum relay networks
Optical fiber coherent link construction
Quantum enhanced spatial and temporal information distribution And gravity sensing
Optical clock with quantum gate operation
Short-range photon network Demonstration experiment
Long-range optical quantum network
Modular ion trap Quantum computer development
Ion trap Quantum computer optical connection
Blind quantum computation
Superconductivity : Long Lifetime Quantum Bit Fabrication Technology
Error tolerant quantum computer
Superconductivity : High-speed, high-precision quantum bit gate operation, quantum bit measurement technology

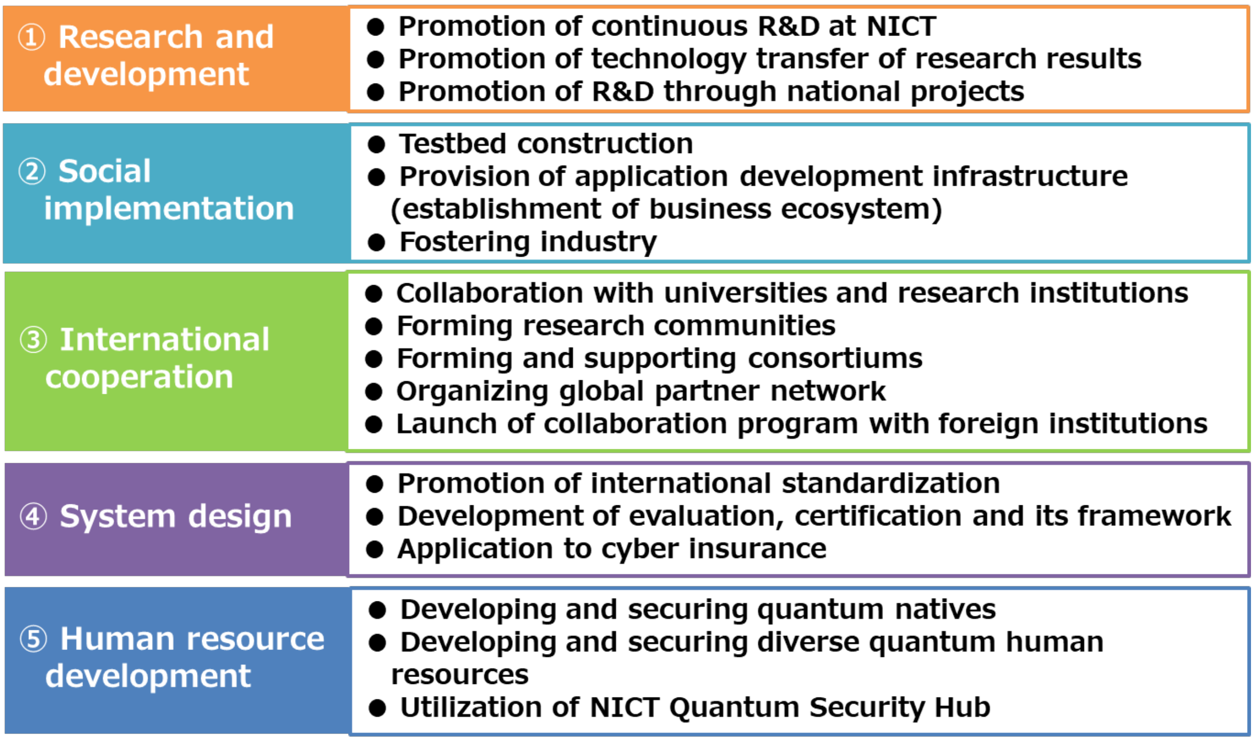
Figure 28 ： R&D Roadmap for quantum network

Chapter 6 : Promotion Strategy

1. Overview

・ Promotion strategy that will be necessary for NICT to develop QKD networks and quantum networks in society in cooperation with external stakeholders.

･In order to deploy quantum networks in society, it is necessary to promote five initiatives in an integrated manner: (1) research and development, (2)social implementation, (3)international collaboration, (4)system design, and (5)human resource development.



① Research and development	● Promotion of continuous R&D at NICT ● Promotion of technology transfer of research results ● Promotion of R&D through national projects
② Social implementation	● Testbed construction ● Provision of application development infrastructure (establishment of business ecosystem) ● Fostering industry
③ International cooperation	● Collaboration with universities and research institutions ● Forming research communities ● Forming and supporting consortiums ● Organizing global partner network ● Launch of collaboration program with foreign institutions
④ System design	● Promotion of international standardization ● Development of evaluation, certification and its framework ● Application to cyber insurance
⑤ Human resource development	● Developing and securing quantum natives ● Developing and securing diverse quantum human resources ● Utilization of NICT Quantum Security Hub

Figure 29 : Promotion strategy for development of quantum networks to society (overview)

2. Individual Promotion Strategy

(1) Research and development

● Promotion of continuous R&D at NICT

・ Based on national plans and strategies as well as NICT's Fifth Medium-to-Long-Term Plan , NICT will work on R&D of quantum network technologies and securing related patents. In fields where it will take five to ten years to achieve research results, we will promote the significance of the research and its results to obtain continuous investment.

● **Promotion of technology transfer of research results at NICT**

・It is necessary for NICT to promote research and development for companies to catch up with the technology in cooperation with the government and other organizations. It is also necessary to operate and improve the system for smoother technology transfer of the basic research results at NICT.

● **Promotion of R&D through national projects**

・ In technology fields where the market size is unclear and it is difficult for companies to participate, such as quantum network technology for which R&D is being promoted mainly in Europe and the United States, it is necessary to promote R&D by establishing a collaboration system among industry, academia, and government through national projects.

(2) Social implementation

● **Testbed establishment**

・NICT will establish an open testbed that connects quantum technology innovation hubs in cooperation with the government, companies, etc., upgrading the Tokyo QKD Testbed (see Initiatives for Building quantum technology Platforms (p61).

・Through the testbed, NICT will combine the achievements of national projects led by government to consolidate and effectively utilize resources in Japan, and establish a framework for joint use among industry, academia, and government.

● **Provision of application development infrastructure (establishment of business ecosystem)**

・NICT will collaborate with governments, companies, the Quantum ICT Forum, and others to provide opportunities to examine and demonstrate new services and use cases at various layers, strengthen application development, and examine business ecosystem models.

● Fostering industry

・NICT will accelerate the diffusion and deployment of quantum networks by promoting R&D and social implementation of quantum networks by telecommunications carriers and service providers.

・To be able to manufacture major devices and parts on quantum networks in Japan, NICT will actively collaborate with related companies such as vendors and component manufacturers in Japan, support the creation of parts manufacturing and business models, and promote the establishment of supply chains. We will also consider the creation of start-up companies from Sony.

(3) International cooperation

● Collaboration with universities and research institutions

・Considering international R&D trends on various quantum technologies, such as ion trap and superconductivity, NICT will collaborate with domestic and oversea research institutes and will also consider applications of the research achievements on quantum communications.

・Toward the realization of quantum networks, NICT will promote collaboration with other universities and research institutions in order to strengthen R&D of quantum relay technology, network architecture, software, etc.

●Forming research community

・NICT will promote the acquisition of research funds by participating in national projects such as the Moonshot Research and Development Program, Q-LEAP, etc., and will also promote the formation of research communities in which participants of national projects and researchers from universities and research institutions participate.

●Forming and supporting consortiums

・NICT will promote collaboration among companies and universities through the Quantum ICT Forum.

・A consortium of quantum technology and Internet researchers from industry, academia, and public research institute has been formed to promote quantum networks, and NICT will participate in and support such an interdisciplinary community.

● **Organizing global partner network**

・ NICT will accelerate the R&D of quantum networks while taking into account the fact that quantum technology is closely related to international cooperation and national security. At the same time, NICT will actively promote the organization of global strategic partners and supporters for standardization in order to build an international testbed.

● **Launch of collaboration program with foreign institutions**

・ NICT will promote discussions on the direction of future R&D and international collaboration, utilizing the framework of collaboration with the EU and NSF.. NICT will strive to make Japanese technology available worldwide while the human and financial resources for R&D on quantum technology are limited.

(4) System design

● **Promotion of international standardization**

・NICT, in cooperation with governments and companies, will promote international standardization at the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC JTC1), for the global spread of quantum network technologies (especially QKD network technologies).

● **Development of evaluation, certification and its framework**

・NICT, in cooperation with the government, companies, the Quantum ICT Forum, etc., will promote the development of appropriate security assessment methods for QKD devices, the documentation of security requirements (so-called Protection Profiles (PPs)) in compliance with international standards developed by ISO/IEC, etc., and the development of an operation framework for PPs.

● **Application to cyber insurance**

・NICT, in cooperation with companies, etc., will consider the application of insurances and reduction of premiums for the introduction of QKD.

(5) Human resource development

● **Developing and securing quantum natives**

・NICT will develop “quantum natives” through the NICT Quantum Camp (NQC) program, started from 2020, in collaboration with governments, universities, companies, etc. NICT will also consider developing human resources who can think in the full stack such as quantum algorithms, high-level programming languages, architecture, etc., as well as human resources who can design the entire system.

・NICT will continue to secure human resources for research by accepting student and adult interns at NICT, expanding collaboration with universities, and developing attractive career paths.

● **Developing and securing diverse quantum human resources**

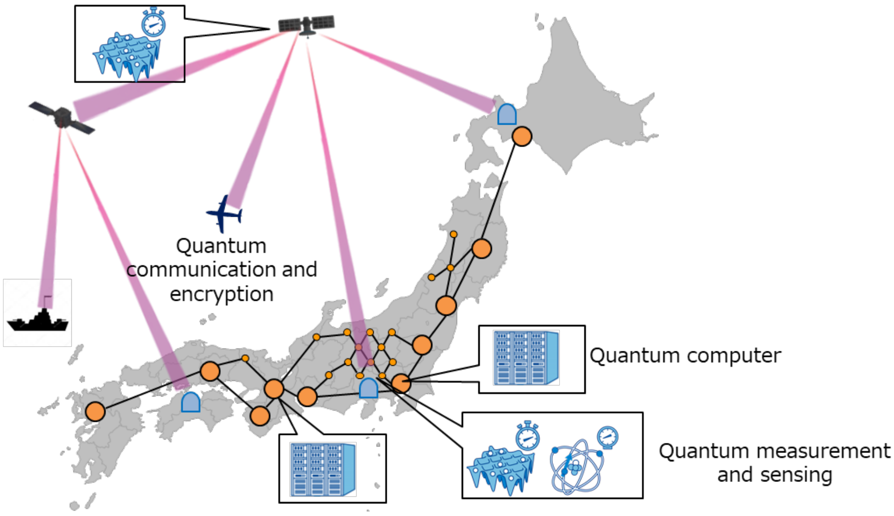
・NICT will secure human resources with various skills not only in research but also in technology, intellectual property management, accounting, etc., in order to strengthen NICT as a research organization.

● **Utilization of NICT Quantum Security Hub**

・NICT will conduct human resource development and hold seminars utilizing the co-creation space at NICT’s new building as the quantum security hub. NICT will also promote practical human resource development programs utilizing open testbed connecting various quantum research hubs.

- Developing quantum network infrastructure connecting each R&D center of quantum technology
- Combining the achievements of national projects to consolidate and effectively utilize resources in Japan, and build a framework for joint use of among industry, academia and government

Stage 1 (around 2022) : Kanto region (quantum computers, quantum cryptography and relay, optical lattice clocks)
Stage 2 (around 2025) : Inter-city (Sendai-city, Tokyo-city, Osaka-city, etc. ; aggregation of quantum technology)
Phase 3 (around 2030) : Integration of satellite and terrestrial networks (throughout Japan)
Phase 4 (around 2035) : Global quantum network



Quantum communication and encryption
Quantum computer
Quantum measurement and sensing

Figure 30 ： Initiatives for building quantum technology platforms

Chapter 7 : Conclusion

- This white paper summarizes the image of society, use cases, elemental technologies R&D roadmap from 2021 to 2035 and promotion strategy on quantum networks.
- With regard to quantum networks, efforts for social implementation of QKD and research and development for the “Quantum Internet” are being internationally promoted. In the future, in accordance with the Fifth Medium-to-Long-Term Plan of NICT and based on the promotion strategy of this white paper, NICT will collaborate with experts, companies, universities, and research institutions in Japan and overseas to promote quantum networks into society.
- In addition, NICT will update on this white paper based on future international trends and R&D progresses.

Reference

(1) Work member list (NICT)

Hitoshi Asaeda, Akie Izumi, Yasuki Ishitani, Shinji Ide, Tetsuya Ido, Toshiyuki Ihara, Hiroyuki Endo, Nozomu Otsubo, Atsushi Kanno, Yoshihiko Saito, Akihiko Sasaki, Masahide Sasaki, Shiho Shono, Norihiko Sekine, Koichi Senba, Masahiro Takeoka, Yoshiro Tsujimoto, Hirotaka Terai, Morio Toyoshima, Nils Nemitz, Hidekazu Hachisu, Kazuhiro Hayasaka, Kentaro Furusawa, Shigeto Miki, Takaya Miyazawa, Kazuhisa Matsuzono, Isao Morohashi, Kotaro Yanagisawa, Yuya Yamaguchi, Fumiki Yoshihara

(2) Update History

- Release 0.9: April 30, 2021

The English text (version 0.9) was translated from the Japanese text (version 1.0) by whitepaper work members using TexTra*, a machine translation system developed by NICT.

＊https://mt-auto-minhon-mlt.ucri.jgn-x.jp/

NICT
National Institute of
Information and Communications Technology

Quantum Network White Paper

Published March 2021
ISBN978-4-904020-14-2

National Institute of Information and Communications
Technology

4-2-1 Nukuikitamachi, Koganei City, Tokyo, 184-8795
E-mailnict-idi-wp@ml.nict.go.jp
URL https://www2.nict.go.jp/idi/