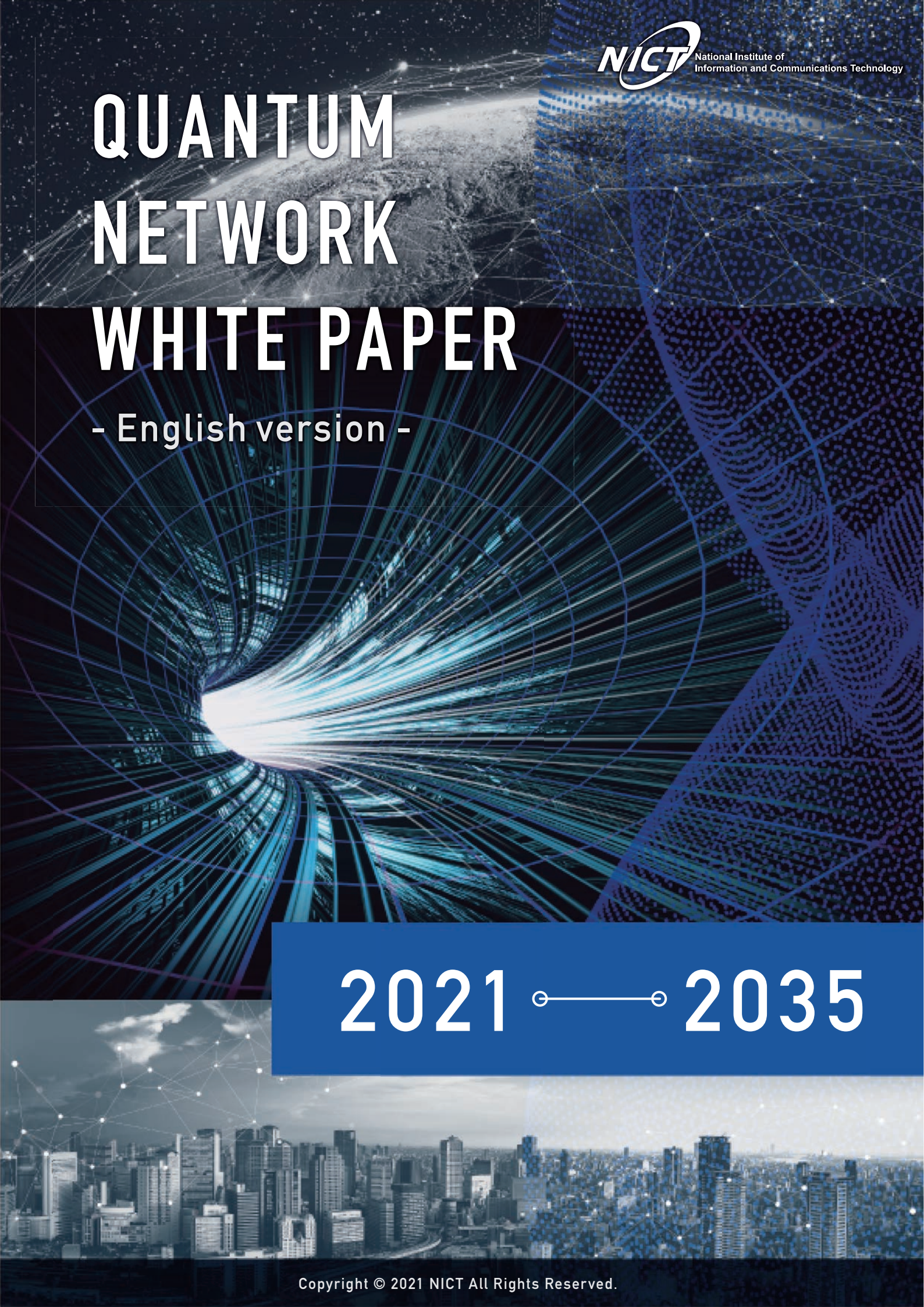


Table of contents

01 CHAPTER.1 INTRODUCTION

1. Background of the White Paper

(1) Objective

• Efforts are under way in Japan and overseas to develop quantum cryptography and quantum networks, with the ultimate goal of achieving 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, and, as the "Quantum Security Hub" in the government's strategy, started work in FY2020 on creating a hub for industry-academia-government collaboration and developing human resources.

• This White Paper describes the direction of NICT's research and development as the hub of quantum security and the issues to be tackled in the future, in order to attract international researchers, promote cooperation with international research institutes, and accelerate research and development of quantum networks.

(2) Overview of the White Paper

• This White Paper outlines international trends in quantum communication, an image of society and potential examples of quantum networks, and an R&D roadmap and NICT's promotion strategy to realize such a society and examples of use. This is the first edition of the White Paper.

• The ultimate goal is to achieve 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 various 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 an overview of quantum information communications

(1) Overview of quantum information communications

• Information and communications technology, such as the Internet, supports the development of the global economy and society, and is a source of industrial competitiveness.

• The digital transformation (DX) is continuing even amid the Covid-19 pandemic, leading to social change through the use of information and communications networks.

• However, cyber-attacks on information and communications networks continue to increase, and therefore secure information and communications infrastructure is required.

• It is feared that the latest cryptography used in modern information and communications networks

01 CHAPTER.1 INTRODUCTION

will be broken by high-performance 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. There is also the risk that attackers could be capturing encrypted data flowing through existing information and communications networks, intending to decrypt the data when high-performance quantum computers become available (harvest now, decrypt later).

• For this reason, quantum cryptography is required to realize "information-theoretic security" that cannot be decrypted by any computer in principle. Several countries such as the United States, European countries, China and Japan, are rapidly conducting R&D, demonstrating practical applications, and constructing quantum cryptography networks for actual operation.

• The Beyond 5G/6G, for which R&D activities have started in various countries around the world, includes "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 under way in Japan and overseas. In the future, these technologies are expected to 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 the so-called "Quantum Internet," in which quantum information devices are connected to quantum networks.

• The Quantum Internet is expected to become a new social infrastructure that provides new applications and services never 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 as well as national security.

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

• Other countries such as the United States, European countries, 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 key technologies and human resource development in order to achieve 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 the "Quantum Internet Blueprint Workshop" (July 2020) to discuss the direction and milestones of research and development for the Quantum Internet.

01 CHAPTER.1 INTRODUCTION

[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 key 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 has exceeded 7,000 km as of 2018. A number of companies have been established to provide communication equipment, devices, and platforms. In addition, China launched the satellite "Mozi" in 2016 and successfully demonstrated a quantum cryptosystem between the satellite and the earth. In January 2021, China demonstrated 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.

• However, these are individual R&D initiatives undertaken by relevant ministries, agencies, and companies, and may not be 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, quantum technology is currently being studied by 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)).

• In 2020, the Cabinet Office started research and development of quantum technologies, including quantum communications, under the "Moonshot Research and Development Program," and the

01 CHAPTER.1 INTRODUCTION

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

-Outline 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 each time, 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.

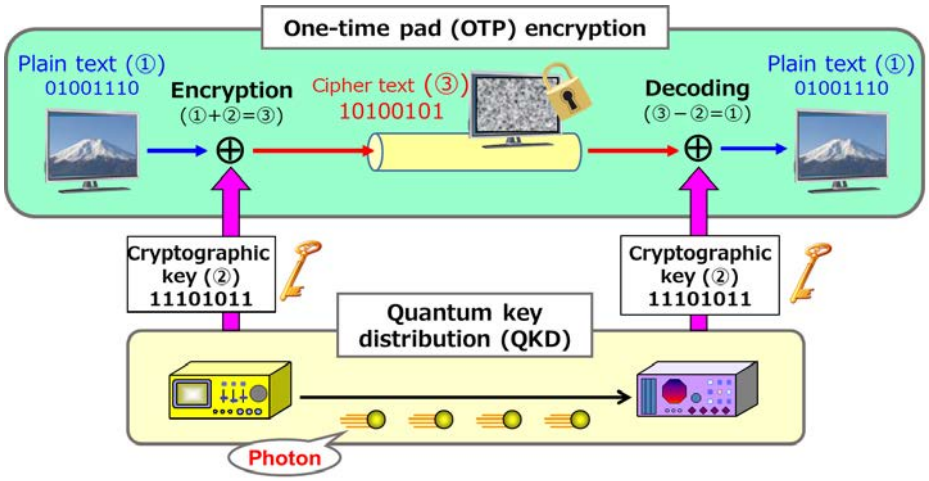


Figure 1 : Mechanism of quantum cryptography

-What kind of system? Why do we need it?-

• The cryptography that is widely used today secures confidentiality in "computational security," which would require a huge amount of computing power to decrypt. 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 then decrypted when new computing technology becomes available in the future.

• On the other hand, quantum cryptography has information-theoretic security: it cannot be decrypted in principle by any computer in the future. At present, the only cryptographic technology that can

01 CHAPTER.1 INTRODUCTION

achieve information-theoretic security is quantum cryptography, which thus offers the strongest level of confidentiality among currently known cryptographic technologies. Quantum cryptography can be used to protect national secrets 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, European countries, the United States, China, and South Korea, and international standardization and full-scale practical application are starting.

-Requirements-

• 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-theoretic secure encryption key are realized.

(4) Quantum network

-Outline of technology-

• A quantum network is 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 (0s and 1s), and is used for various applications.

• Distribution of quantum information through a quantum network is expected to enable quantum cryptography over longer distances than is 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 key 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-

• To realize a quantum network, the following key technologies are required: quantum memory technology for storing and processing quantum information; quantum interface technology for connecting optical signals and quantum memory; and quantum repeater technology for relaying and transmitting

01 CHAPTER.1 INTRODUCTION

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 materials and candidate relay methods.

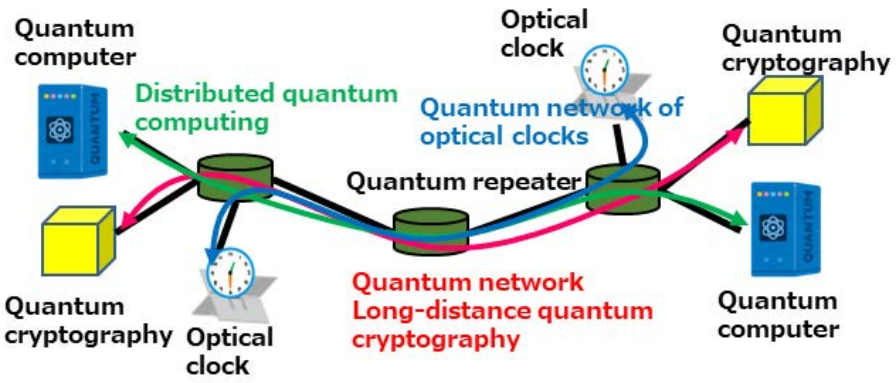


Figure 2 : Overview of quantum networks

(5) Quantum Internet

• Definitions of the Quantum Internet are shown 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 that connects quantum information equipment and devices such as quantum computers and quantum sensors. Also, given that the current Internet is a network in which multiple networks are interconnected and digital information (bits) is distributed, the Quantum Internet is a network in which multiple quantum networks are interconnected and quantum information (qubits) is distributed.

• In the future, the definition of the Quantum Internet is expected to be clarified through international discussions as its key technologies mature.

• When the Internet first appeared, no one imagined that it would become indispensable infrastructure for socio-economic activities and people's lives. Today, it is not clear what kind of network the Quantum Internet will be and how it may be used. However, it is expected to be used for future applications and services that cannot be imagined at present, and to make people's lives richer, safer and more secure.

01 CHAPTER.1
INTRODUCTION

	Document/Organization	Example of definition
United States	"A Strategic Vision for America's Quantum Networks" (Feb.2020), National Quantum Coordination Office, White House	The quantum internet—a vast network of quantum computers and other quantum devices.
	"Quantum Internet Blueprint Workshop" (Oct.2020), 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.
Europe	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.
	"Strategic Research Agenda on Quantum Technology"(Mar.2020), 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.
Standardization Body	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.

Table 1 : Example definitions of the Quantum Internet

02 CHAPTER.2
IMAGE AND USE CASES OF QUANTUM NETWORKS IN SOCIETY

1. Image of society with quantum networks

(1) Overview

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

• In the 2020s, QKD networks are expected to enable the 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 that interconnect 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 entirely new applications and services will emerge. The Quantum Internet is expected to provide the foundation for affluent lives and socioeconomic activities.

	Examples of use cases	Progress in quantum network technology	Quantum computing and sensing technologies
2020s	● 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 would have a significant impact on corporate activities due to leakage of trade secrets, know-how, important technologies, etc. ● Finance : Exchange of information on financial systems, transactions, etc.	• QKD (Kanto region → nationwide)	• NISQ Quantum Computer IBM[1] 2020 : 65qubit 2021 : 127qubit 2022 : 433qubit 2023 : 1121qubit
2030s	● Administration/Diplomacy/Security : Exchange of personal information in administration, communication of confidential 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 (nationwaide → global) • Satellite QKD/physical layer encryption • Quantum networks	• NISQ Quantum Computer • Small-scale fault-tolerant quantum computers • Quantum sensors
2040s	★ 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 the Shannon limit)	• QKD (global scale) • Satellite quantum communication • Quantum networks (global scale)	• Fault-tolerant quantum computers • Distributed quantum computing • Quantum sensors

● : QKD, ★ : Quantum computer, ▲ : E quantum sensing

Table 2 : Examples of Use Cases of Quantum Networks

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

02 CHAPTER.2
IMAGE AND USE CASES OF QUANTUM NETWORKS IN SOCIETY

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 would have a significant impact if leaked, must be protected for a long time. When sending such information over a network, it is expected that QKD, which guarantees information-theoretic security, will be used.

Information holder	Examples of information to be protected
National/local governments	• Information related to diplomacy, defense, security, geographic (infrastructure, underground space), family registers/residents, voting, etc.
Organizations (enterprises, etc.)	• Customer lists, new business plans, prices, response manuals, other sales information • New technologies, manufacturing methods, know-how, design drawings, other technical information
Individuals	• Health data, genome information, 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 medicine, industry, services, government, diplomacy, security, and daily life.

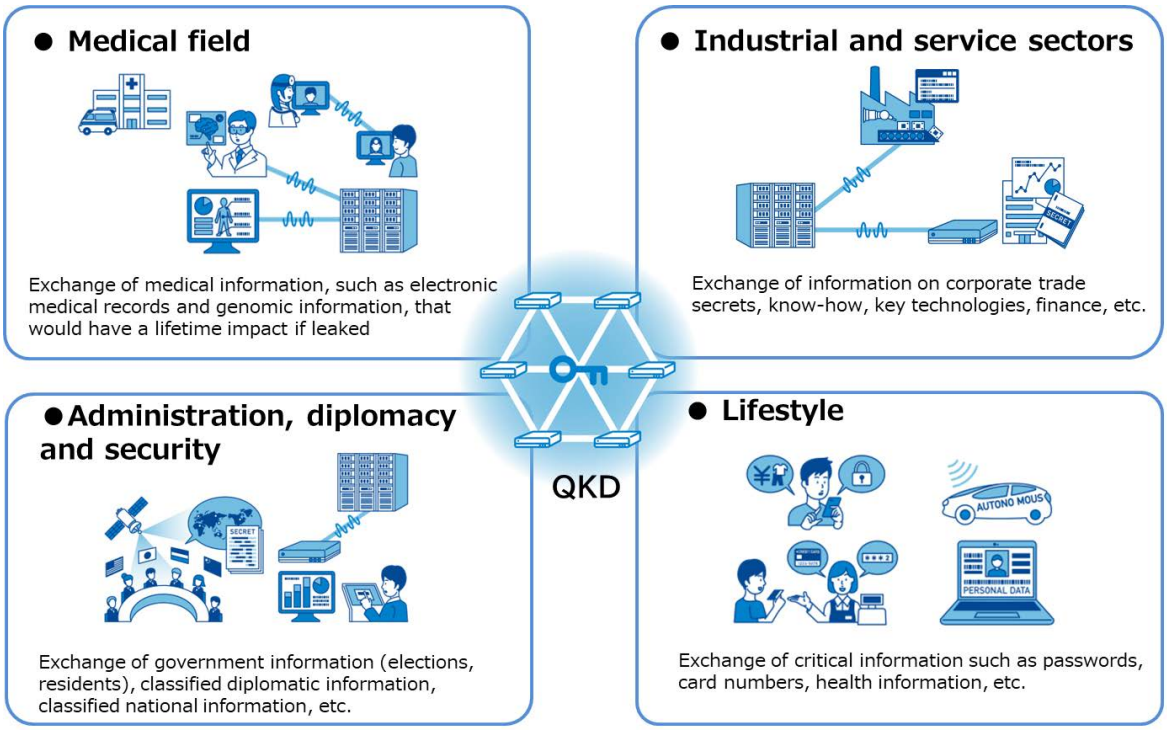


Figure 3 : Examples of use cases realized by QKD

02 CHAPTER.2
IMAGE AND USE CASES OF QUANTUM NETWORKS IN SOCIETY

(3) Examples of use cases in individual fields

① Medical and financial fields – secure distribution, storage and utilization of data in the quantum secure cloud

【 Background and necessity 】

• It is important to store large amounts of information, which is an important management resource of a company, using encryption and other methods, and to decrypt them properly when 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 can never be broken is required.

【 Outline of technology 】

• Quantum secure cloud technology is a cloud technology that enables the 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 requires enormous computational power 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 prevents tampering and decryption, 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.

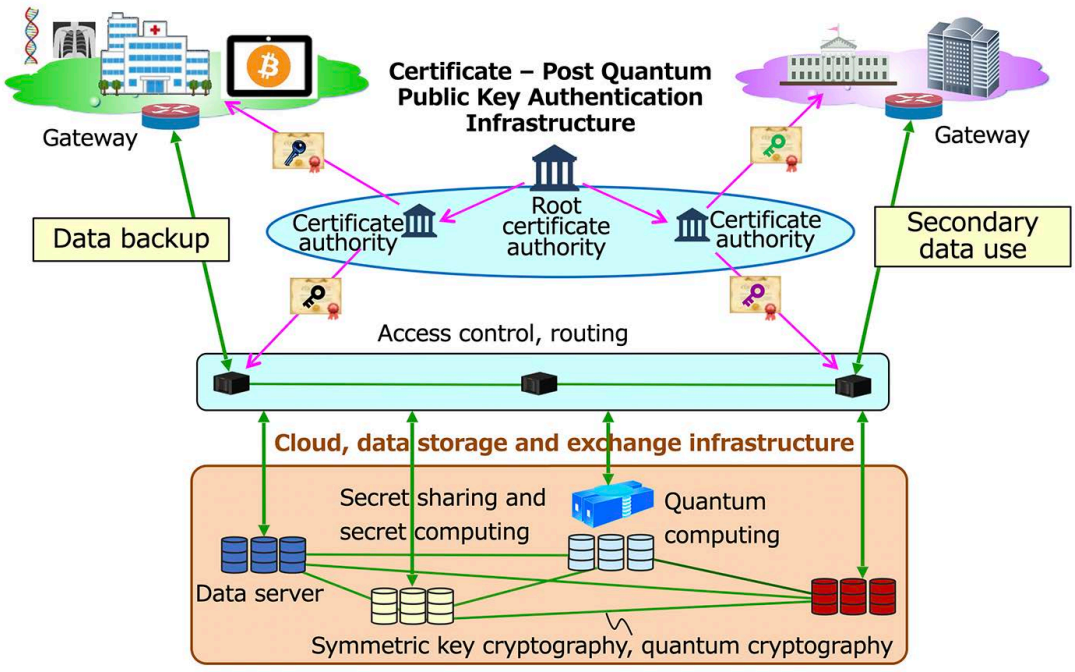


Figure 4 : Mechanism of quantum secure cloud technology

02 CHAPTER.2
IMAGE AND USE CASES OF QUANTUM NETWORKS IN SOCIETY

② Administration, diplomacy and security – Secure backbone network with satellite QKD

【 Background and necessity 】

• The QKD network needs to spread widely across Japan and other countries in order to securely exchange information related to national security and confidentiality, as well as personal information held by local governments.

• However, QKD is inherently vulnerable to signal attenuation, which makes long-distance transmission of quantum cryptography using optical fiber difficult. Therefore, satellite-based quantum cryptography communications networks in space, in which signal attenuation is less than that of optical fibers, will play an important role in realizing a global-scale QKD network.

【 Outline of technology 】

• 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.

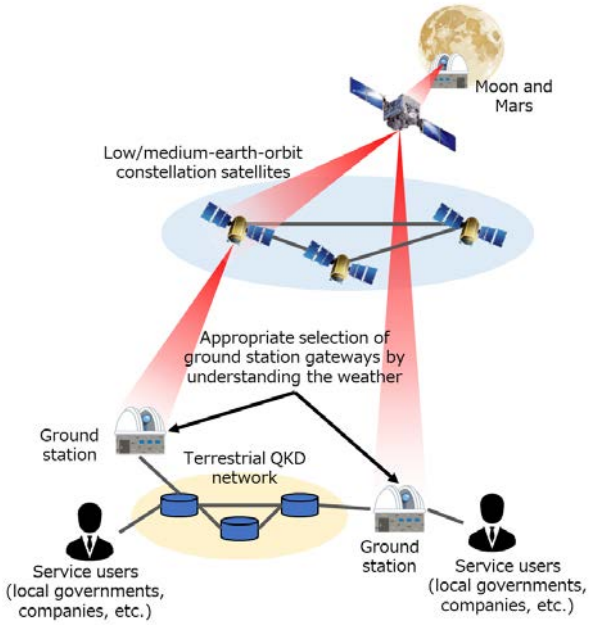


Figure 5 : Secure backbone network with satellite QKD

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 in the industrial and service sectors have accumulated over many years are important information. One way to prevent the information leakage this information by industrial espionage is to use a local secure network

02 CHAPTER.2
IMAGE AND USE CASES OF QUANTUM NETWORKS IN SOCIETY

based on free space optical (FSO) communication, which can be built independently by companies on the scale of their premises, office buildings, and major branch offices.

【 Outline of technology 】

・A secure network that can be built independently by companies must be able to be: (1) built independently of external organizations, and (2) 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 using the equipment and components used in current optical communications, can be implemented in FSO communications. By implementing this system in FSO communications, a secure network that satisfies the above requirements can be built without procuring and installing new optical fibers. In addition, by combining this system with physical layer cryptography(see Chapter 4), which utilizes a unique characteristic of FSO communications, namely that the spatial divergence of laser light is narrower 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.

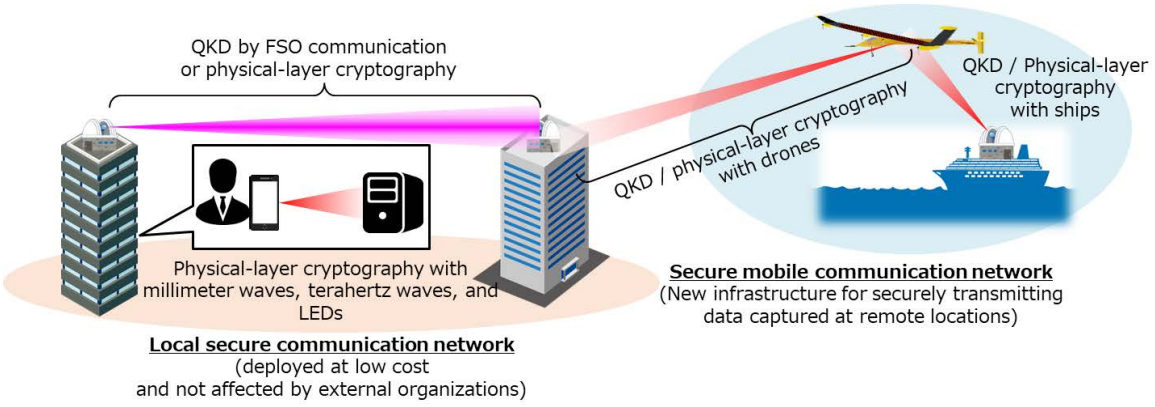


Figure 6 : Local secure network with QKD and physical layer encryption

④ Daily life – Highly secure infrastructure available to everyone

【 Background and necessity 】

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

・Therefore, the security technology used in the current security infrastructure is required to be updated.

【 Outline of technology 】

・In this infrastructure, key exchange and authentication on a classical network is carried out by 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,

02 CHAPTER.2
IMAGE AND USE CASES OF QUANTUM NETWORKS IN SOCIETY

enhancing the security of networks. Since these technologies can be implemented as algorithms on mobile terminals, individuals can use this infrastructure easily.

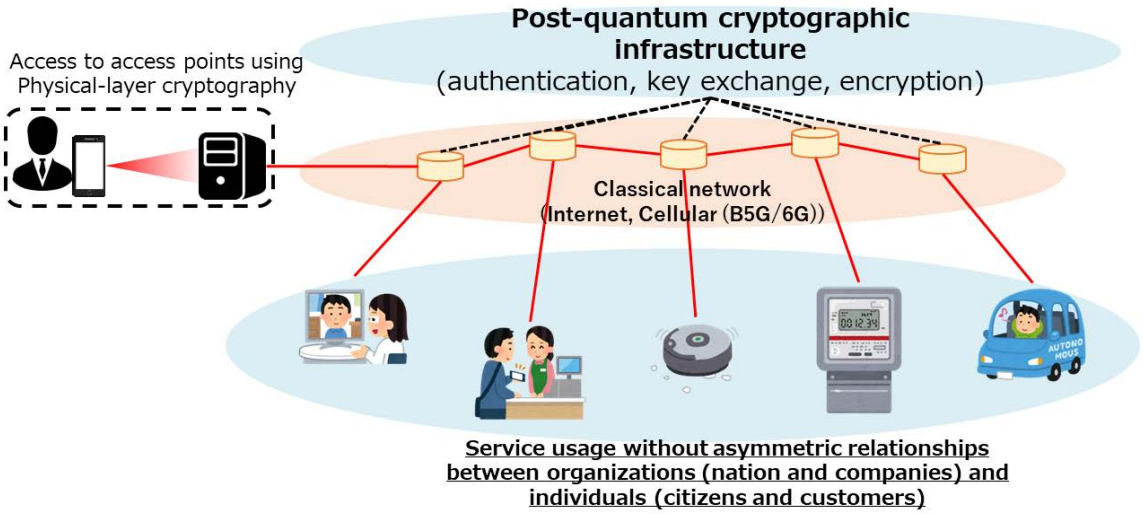


Figure 7 : New security infrastructure with post-quantum cryptography infrastructure

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

(1) Image of society and use cases

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

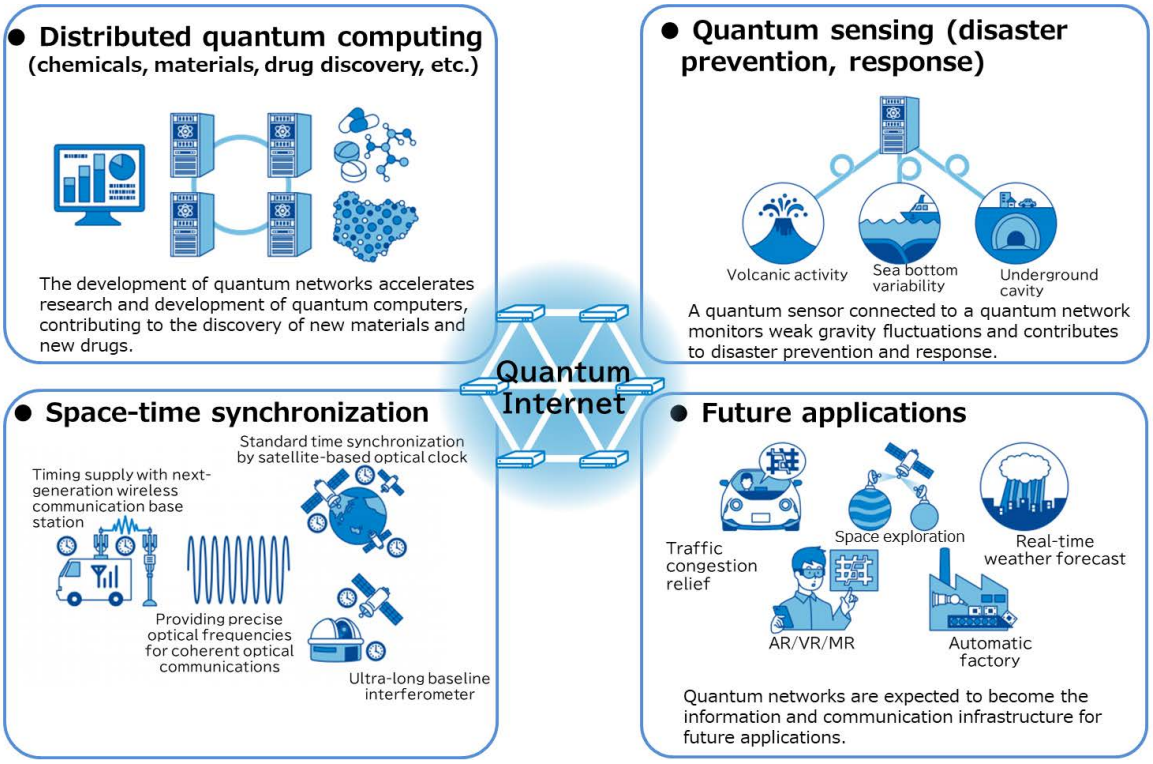


Figure 8 : Examples of society and use cases realized by quantum networks

02 CHAPTER.2
IMAGE AND USE CASES OF QUANTUM NETWORKS IN SOCIETY

(2) Examples of use cases in specific fields

① Quantum sensing – disaster prevention and disaster response

【 Background and necessity 】

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

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

【 Outline of technology 】

• 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 needed. A coherent link compares and synchronizes optical clocks by connecting their optical frequencies as light waves. A quantum network of optical clocks will enable the fastest measurement of the optical frequencies of the clocks allowed by physics by adding it to the coherent link.

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

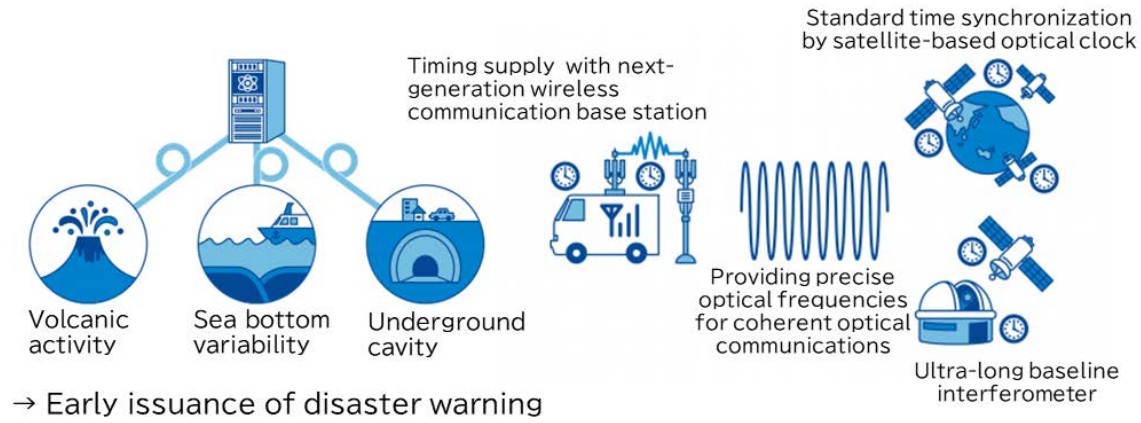


Figure 9 : Use cases of quantum networks for optical clocks

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 are 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

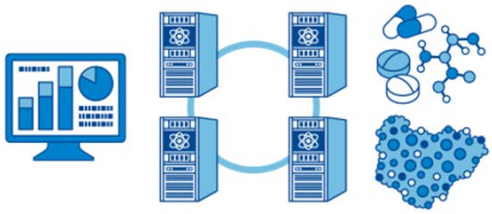
02 CHAPTER.2
IMAGE AND USE CASES OF QUANTUM NETWORKS IN SOCIETY

method of performing quantum computation while keeping the computation secret is required. By using a small-scale quantum computer connected to a large-scale quantum computer by a quantum network, such blind quantum computation is expected to be possible.

【 Outline of technology 】

• Quantum computing is a computational method that uses quantum bits (qubits) based on quantum physics instead of classical digital bits (0s and 1s) 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 is required. These include 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.



The 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

03 CHAPTER.3
QUANTUM NETWORK EVOLUTION

• This chapter describes the predicted evolution of quantum networks by the 2025s, 2030s, and 2040s.
• Quantum networks using QKD and quantum repeaters will be introduced in stages as the technology is developed and implemented. However, this 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 networks and quantum networks will coexist. Such coexistence will enable the various services described in the previous chapter. The following is an overview of the predicted evolution of quantum networks.

1. Image around the year 2025

• The quantum key distribution (QKD) network between the ground and satellites will start operation, providing a secure communication service. Services using quantum computing and quantum sensing using classical networks will also be launched.

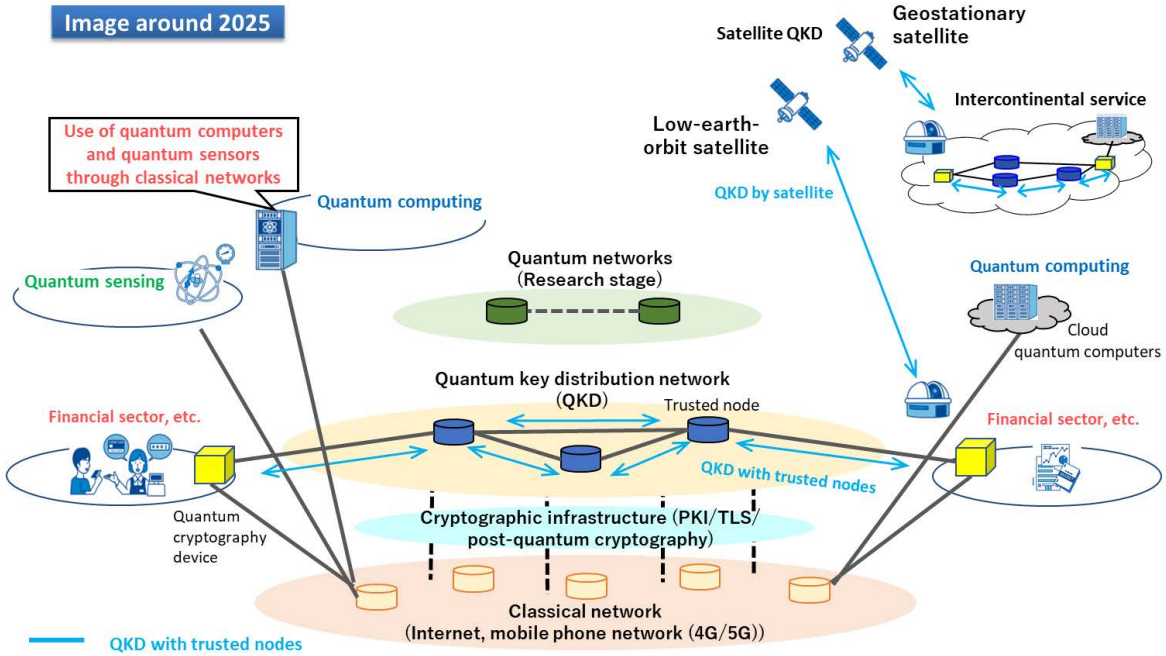


Figure 11 : Evolution of quantum networks around 2025 [2]

2. Image around the year 2030

• The operation of QKD networks connecting the ground and satellites by secure communication services will expand. Services using quantum computing, quantum measurement and sensing over classical networks will also expand.

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

03 CHAPTER.3
QUANTUM NETWORK EVOLUTION

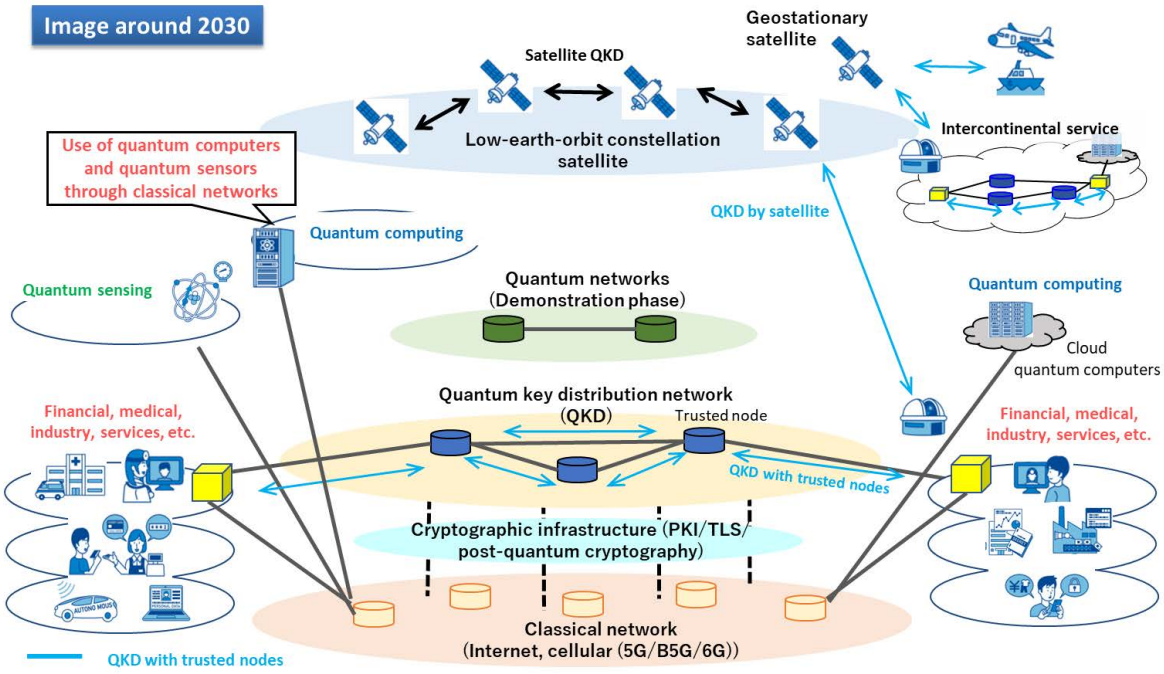


Figure 12 : Evolution of quantum networks around 2030

3. Image around the year 2040

・A global quantum network of satellites and terrestrial networks will be established, and virtual quantum network services will be realized, accommodating a wide variety of quantum networks and protocols.

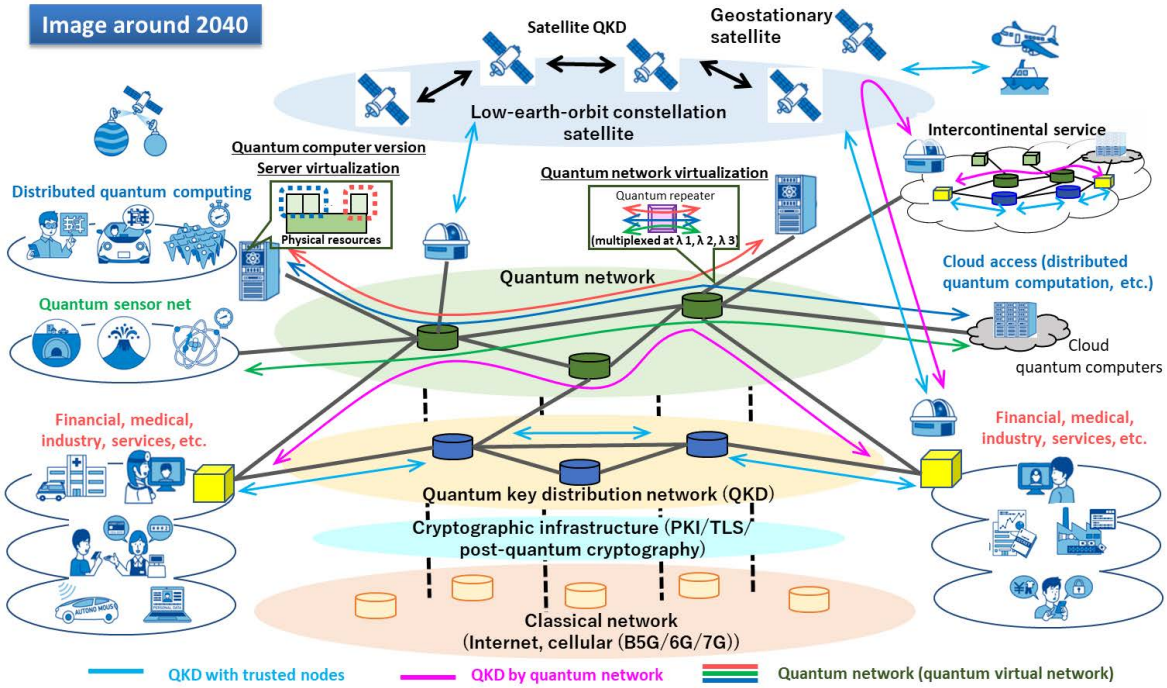


Figure 13 : Evolution of quantum networks around 2040

03 CHAPTER.3
QUANTUM NETWORK EVOLUTION

• Infrastructure providers and quantum virtual network operators (VNOs) will construct virtual quantum networks and provide services to meet the needs of application/content providers using quantum networks around 2040.

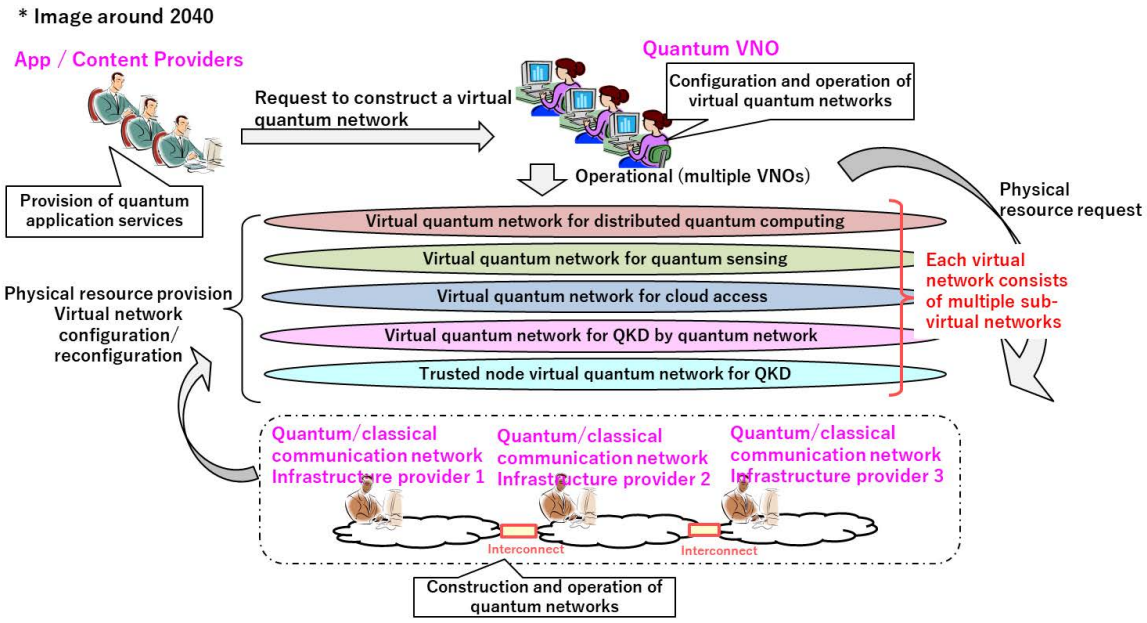


Figure 14 : Image of quantum network services around 2040

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

1. Overview of quantum network technology

(1) Overview of key technologies

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

Quantum communication and cryptographic link technology

Terrestrial link (NICT)
- Increase the speed of current protocols and improve implementation safety
- Longer distance, CV-QKD technology
- Advancement of security technology

Satellite link (NICT)
- Quantum cryptography for satellites
- Advanced tracking technology, ultra-high sensitivity and low-loss optical transmission/reception antennas

Quantum communication device (NICT)
- 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

Peripheral technology (NICT)
- Thermal noise random number source
- Stable supply of high-performance single-photon detection devices
- Extension of device-independent QKD theory, etc.

NICT indicates a technology area related to NICT.
Technology themes in red color indicate NICT's initiatives.

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

Quantum network 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 related to NICT.
Technology themes in red color indicate NICT's initiatives.

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

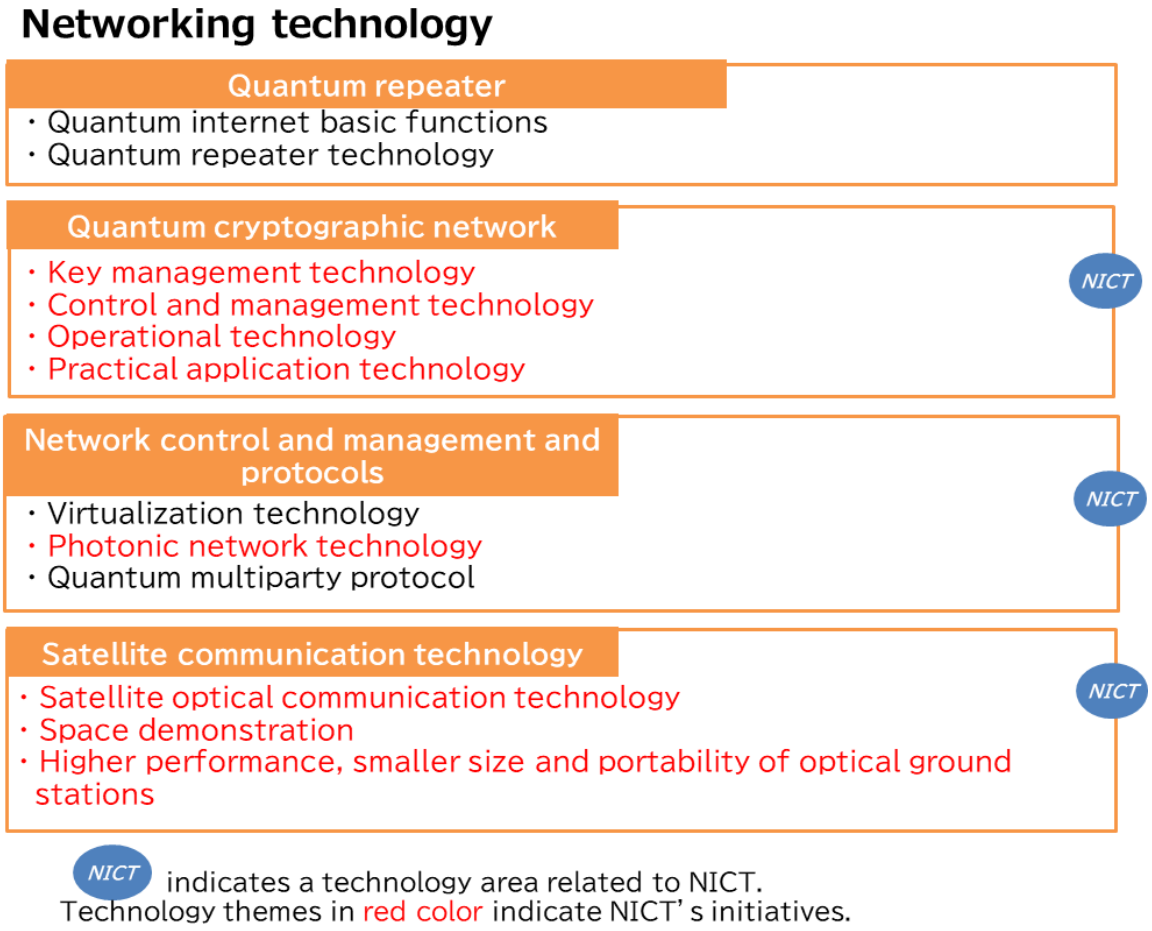


Figure 15 : Overview of quantum network technologies

(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 key technologies and requirements.

04 CHAPTER.4
KEY 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
	② Physical layer encryption technology
	③ Satellite/ground network coordination technology
(3) Quantum network	
	① Quantum interface
	② Quantum repeater
	③ Multi-quantum network control & management
	④ Quantum sensor network (Quantum network of optical clocks)
	⑤ Quantum computing (Ion trap quantum computer)
	⑥ Quantum computing (Superconducting quantum computer)

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

2. Key technologies and requirements

(1) Quantum key distribution (QKD) network

【 Overview 】

・A QKD network is a technology that makes it possible to share cryptographic keys with 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 communications network, etc.) in which several application services are provided. In other words, by adding a QKD network to a conventional network, it is possible to provide a secure cryptographic key for a very long time. One of the applications of the QKD network is quantum secure cloud technology.

【 Required technologies 】

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

【 International trends 】

・Demonstrations and test operations are under way 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 been operating the longest in the world.

As for QKD modules, ID Quantique (Switzerland), Quantum CTek (China), Toshiba (Japan) and others have started commercialization and operation, and NEC (Japan) is now conducting field tests. 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

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

Quantum Xchange (USA). Incumbent telecommunications companies such as BT (UK), Verizon (USA), and SK Telecom (Korea) are also entering the market.

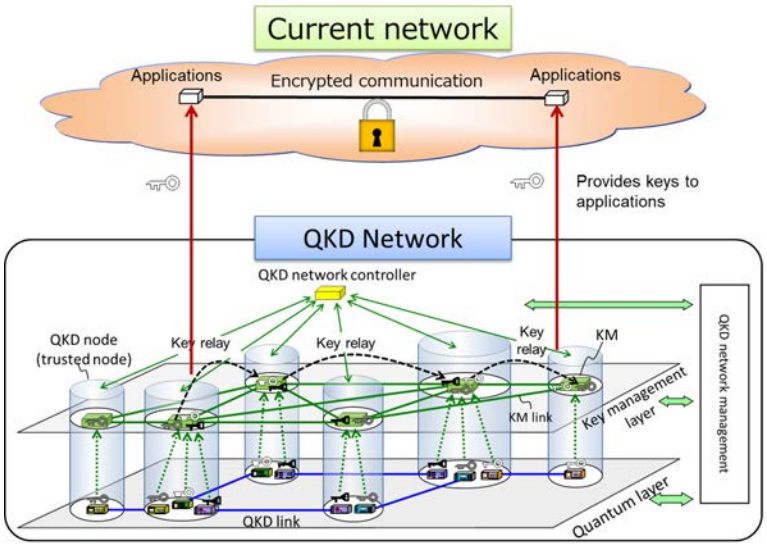


Figure 17 : QKD network configuration

【 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 a framework for evaluation, testing, and certification 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.

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

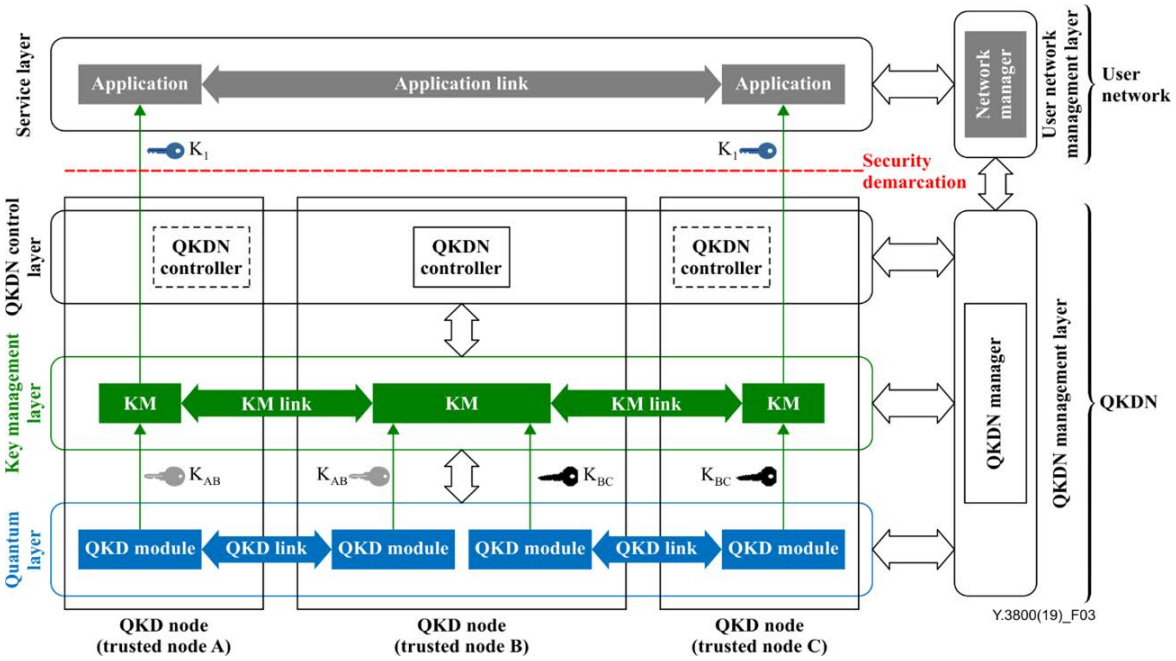


Figure 18 : Basic configuration of the QKD network specified in ITU-T Y.3800 [3]

• The key technologies required for QKD networks, their applications, quantum secure cloud technology are outlined below.

① Quantum key distribution (QKD)

【 Outline of technology 】

• This technology is used to share encryption keys between two distant parties using photons, which are particles of light. Due to the uncertainty principle of quantum mechanics, any eavesdropping attack on photons can be detected without fail. By using cryptographic keys that cannot be eavesdropped, information-theoretic 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 QKD transmitter/receiver pair can generate a key is currently limited to 50–100 km at the most.

② Key management and key relay technology

【 Outline of technology 】

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

3. QKDN: QKD Network, KM: Key Manager

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

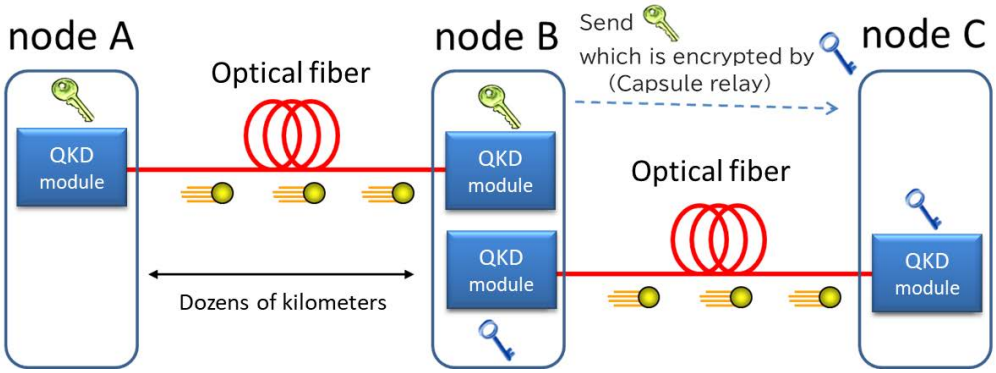


Figure 19 : Key relay mechanism in QKD network

③ QKD network control and management technology

【 Outline 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

【 Outline 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 channel using quantum cryptography to form a storage network, and secret sharing algorithms are implemented on the network to realize information-theoretic 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 in case 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 contained in the meaningless distributed data.

• User authentication and data falsification prevention are performed using certificates with digital signatures issued by the post-quantum - public key authentication infrastructure. This 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

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

on quantum secure clouds, the post-quantum - public key authentication infrastructure is used 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.

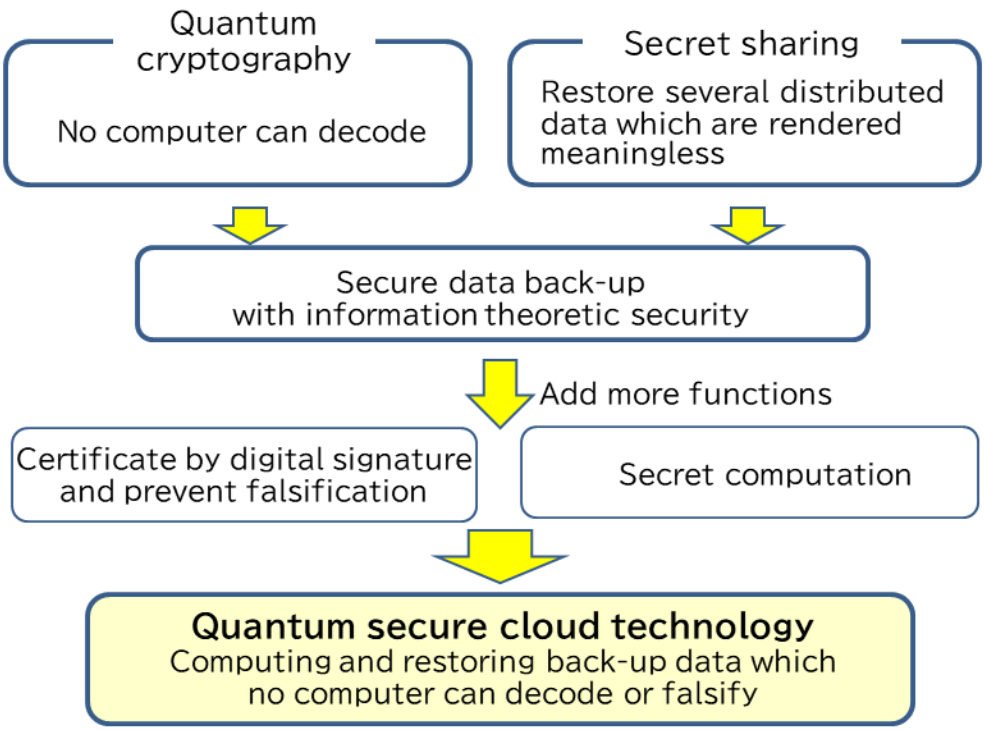


Figure 20 : Quantum secure cloud technology

【 What kind of system? Why do we need it? 】

・This technology is necessary to ensure ultra-long-term confidentiality of data, including medical information such as patient information and genetic data. On the other hand, there is concern about data loss due to disasters, etc., in case such data is stored in only one hospital. It is also crucial to safely back up data in remote locations. The quantum secure cloud can meet both these needs. (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 】

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

04 CHAPTER.4 KEY TECHNOLOGIES AND REQUIREMENTS

(2) Satellite and FSO communications

① Satellite quantum key distribution (QKD) technology

【 Outline of technology 】

• This technology provides an information-theoretic secure method to share cryptographic keys through quantum communication between the ground and a satellite, or between satellites. (See "Secure backbone network with satellite QKD" on p. 21.)

【 What kind of system? Why do we need it? 】

• In terrestrial QKD networks, the optical loss of optical fibers sets a limit on the transmission distance of QKD. So a huge number of QKD devices and trusted nodes are required for globalization. On the other hand, the thickness of the atmosphere 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 successfully conducted a QKD experiment[5]between a low-earth orbit satellite and the ground. Research on satellite QKD is accelerating among governments, universities, and venture companies around the world.

【 Requirements 】

• 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. Moreover, high-speed and high-sensitivity single-photon detector technology to detect photons is required.

② Physical layer encryption

【 Outline of technology 】

• Unlike QKD, which is secure against any physically possible attack, physical-layer cryptography provides an information-theoretically secure method for key establishment under the restrictions on eavesdropper's attack models, such as when eavesdroppers eavesdrop from the outside of the line-of-sight between the sender and receiver. (See "Secure backbone network with satellite QKD" on p. 21, "Local secure network with QKD and physical layer encryption" on p. 22, and "New security infrastructure with post-quantum cryptography infrastructure" on p. 23.)

【 What kind of system? Why do we need it? 】

• 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.

4. H. Takenaka, et al., Nat. Photonics (2017)
5. S.–K. Liao, et al., Nature (2017)

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

【 International trends 】

・ NICT is conducting a series of researches on physical-layer cryptography in free-space optical communications.[6] Companies and universities dealing with QKD have applied for patents on similar concepts.[7]

【 Requirements 】

・ 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. 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)

【 Outline 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 the weather. (See “Secure backbone network with satellite QKD” on p. 21.)

【 What kind of system? Why do we need it? 】

・ For example, when satellite QKD/physical-layer cryptography cannot be provided due to 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. NICT has been conducting R&D on this technology.[8]

【 Requirements 】

・ 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 of ground stations on ships in order to establish links with satellites at various locations on the ground.

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)
8. K. Suzuki, ICSO2014, or OBSOC

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

(3) Quantum network

① Quantum interface

【 Outline of technology 】

• This technology is used to transmit quantum information between different quantum physical systems without changing the quantum information. It is also called quantum media conversion.

【 What kind of system? Why do we need it? 】

• 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 】

• A technique for manipulating quantum entanglement is required to generate quantum correlations between the quantum system of matter 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, and the measurement of interference and the manipulation into a quantum system of matter are performed.

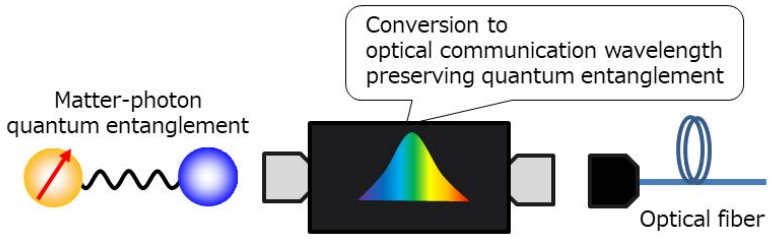


Figure 21 : Role of the quantum interface

② Quantum repeater

【 Outline of technology 】

• This technology enables quantum information to be transmitted over long distances by placing multiple quantum-connected nodes at relay points.

【 What kind of system? Why do we need it? 】

• In principle, quantum states cannot be replicated, so signal attenuation due to loss in the communication channel cannot be recovered by amplification. Therefore, quantum repeaters are

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)

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

necessary to extend the distance of quantum connections. It can also be used 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 under way. 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 under way.[14]

【 Requirements 】

・ In addition to techniques for controlling quantum entanglement 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.

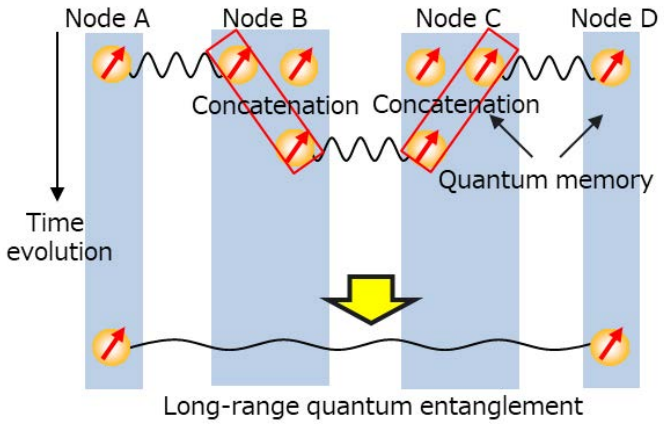


Figure 22 : Mechanism of quantum repeaters

③ Multi-kind quantum network control and management

【 Outline 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 of various future applications, including QKD networks, on the same physical network.

【 What kind of system? Why do we need it? 】

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

12. Nature Photonics 10, 381 (2016)
13. Nature Communications 6, p. 6787 (2015)
14. Nature Communications 10, 378 (2019); Nature Photonics 13, 644 (2019)

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

【 International trends 】

• The ITU-T SG13 is currently discussing software-defined network control (SDN control) and virtualization for QKD networks,[15] while the IRTF is discussing the Quantum Internet (quantum networks).[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 the White House Office of Science and Technology Policy (OSTP) has published a report on the National Strategy of Quantum Information Science.[16] In Europe, the Delft University of Technology in the Netherlands has published a report on future quantum networks, including the Quantum Internet.[17]

【 Requirements 】

• In order to construct virtual quantum networks that satisfy the requirements 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. This will enable the networks to enhance the stability of applications.

• Moreover, applying policy control (e.g.: SDN) and in-network computing technologies (e.g.: information-centric networking and network coding[18]), which have been actively researched and developed in classical networks, is expected to be effective.

• In addition, advanced security technologies will be needed to ensure the safety and security of control and management mechanisms, as well as the integration of terrestrial and satellite-based network technologies to realize global virtual quantum networks in the future.

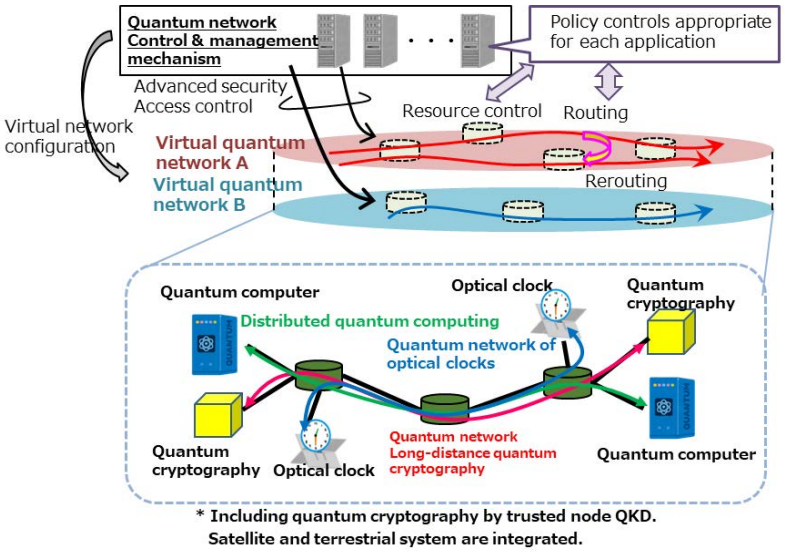


Figure 23 : Mechanism of quantum networks

④ Quantum sensor network (e.g.: quantum network of optical clocks)

【 Outline of technology 】

• Devices that use quantum effects to measure physical quantities are called quantum sensors. Atomic clocks that use optical frequencies are called optical clocks, and they are also used as

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)
16. "Quantum Frontiers: Report on Community Input to the Nation's Strategy for Quantum Information Science," The White House National Quantum Coordination Office (October 2020)
17. "Creating the Quantum Future – QuTech Annual Report 2019," Delft Univ. of Tech. (March 2019)
18. K. Matsuzono, et al., "Low Latency Low Loss Streaming using In-Network Coding and Caching," Proc. IEEE Infocom (May 2017)

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

quantum sensors to measure gravity. Coherent links that connect optical clocks with optical fibers or free space enable the 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.

【 What kind of system? Why do we need it? 】

• The technology is essential 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 may 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 2,000 km is in progress in Europe.[19] 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.[20] To date, the quantum network of optical clocks has merely been proposed; there has been no report on actual implementation.[21]

【 Requirements 】

• 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.

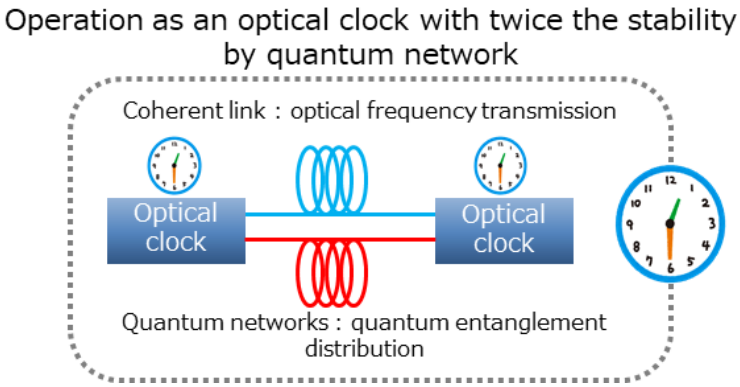


Figure 24 : Quantum network of optical clocks

⑤ Quantum computing (ion-trap quantum computer)

【 Outline of technology 】

• An ion-trap quantum computer consists 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.

19. https://www.clonets.eu/clonets-consortium.html
20. Optics Express 28, 9186 (2020)
21. Nature Physics 10, 583 (2014)

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

【 What kind of system? Why do we need it? 】

・An 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 United States 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.[22] An ion-trap quantum computer with optical connectivity has not yet been realized, and research and development are under way in the United States and Europe with the goal of achieving 50 qubits.[23] In Japan, research and development has begun under the Moonshot Research and Development program.[24]

【 Requirements 】

・A highly functional ion trap with a quantum interface with photons that can perform quantum computation with about 10 qubits is needed. 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.

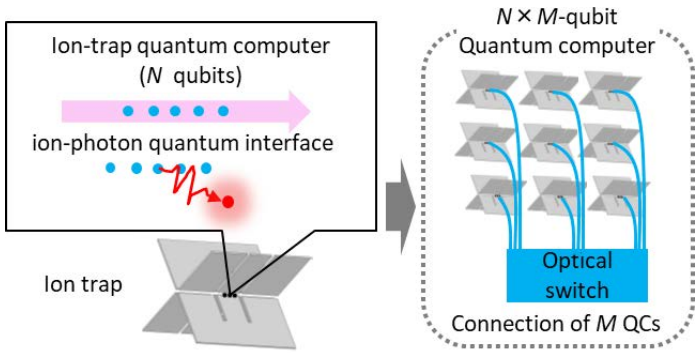


Figure 25 : Optically connected ion-trap quantum computer

⑥ Quantum computing (superconducting quantum computer)

【 Outline of technology 】

・Superconducting electric circuits cooled to cryogenic temperatures behave quantum mechanically, and 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 consisting of a large number of qubits capable of qubit gate operation and state measurement.

【 What kind of system? Why do we need it? 】

・Quantum computers are much more powerful than present computers at solving certain classes of problems by deploying quantum mechanical resources to computation. Superconducting quantum

22. https://ionq.com/, https://www.aqt.eu/
23. https://www.aqtion.eu/
24. https://www.jst.go.jp/moonshot/en/program/goal6/

04 CHAPTER.4
KEY TECHNOLOGIES AND REQUIREMENTS

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.[25] Thus, research and development of NISQ (noisy intermediate-scale quantum computers)[26], a superconducting quantum computer consisting of several tens of qubits without error correction, is actively being conducted. In Japan, the Q-LEAP Flagship project[27]and the Moonshot Research and Development program[28] are conducting research and development.

【 Requirements 】

• 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.

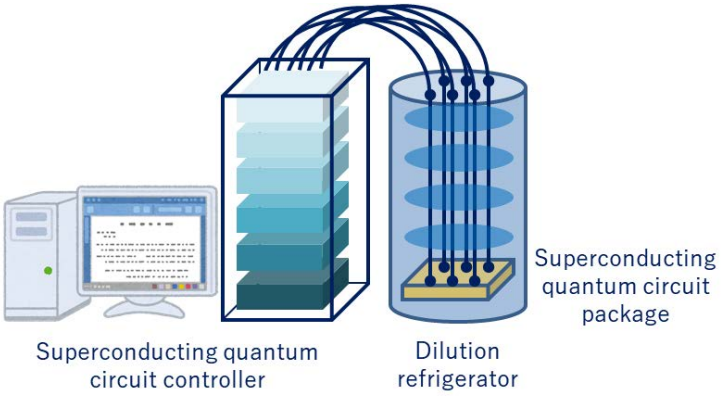


Figure 26 : Superconducting quantum computer

25. https://www.nature.com/articles/s41586-019-1666-5
26. https://doi.org/10.22331/q-2018-08-06-79
27. https://www.jst.go.jp/stpp/q-leap/en/index.html
28. https://www.jst.go.jp/moonshot/en/program/goal6/

05 CHAPTER.5
R&D ROADMAP

• For the key 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.

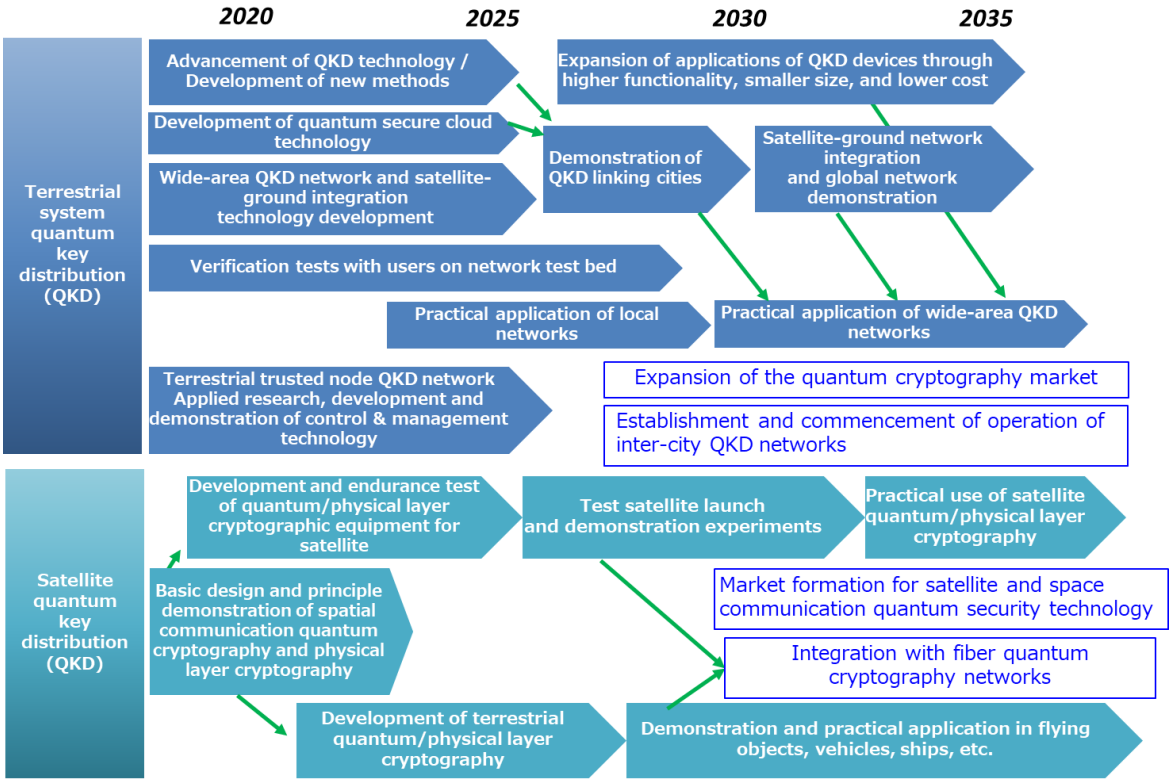


Figure 27 : R&D Roadmap for QKD networks

05 CHAPTER.5
R&D ROADMAP

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

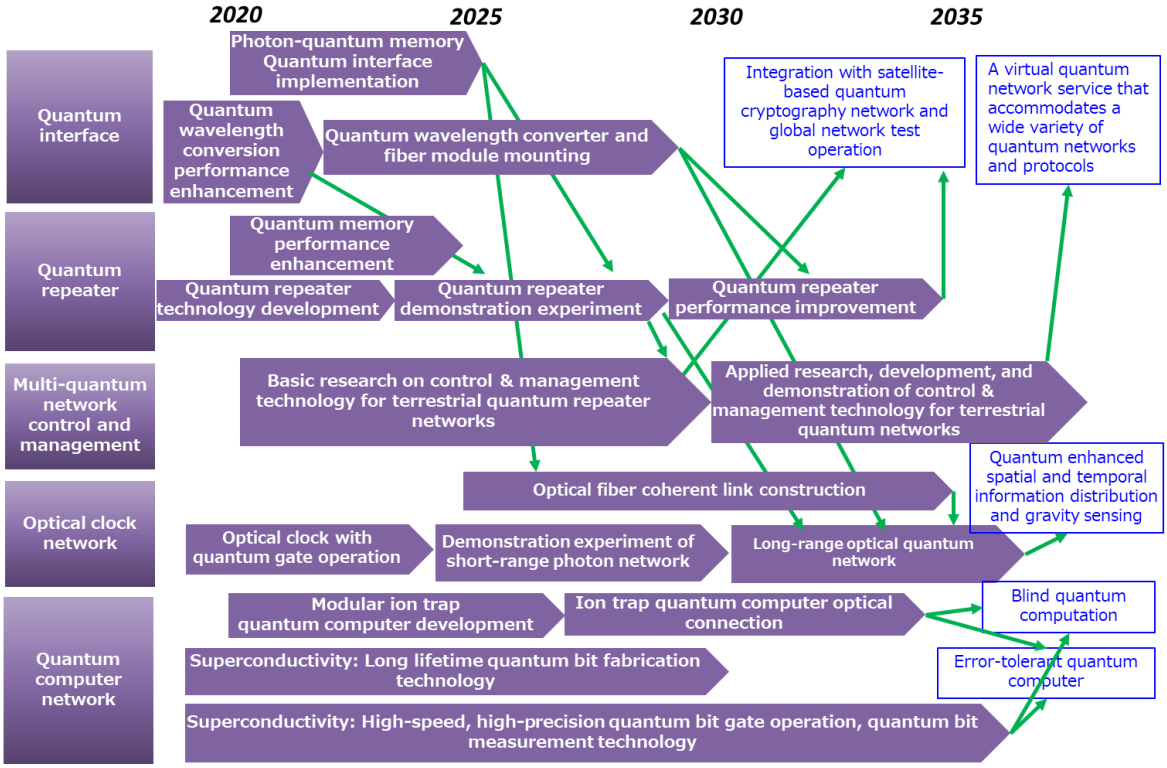


Figure 28 : R&D Roadmap for quantum networks

06 CHAPTER.6 PROMOTION STRATEGY

1. Overview of quantum network technology

・A promotion strategy 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	● Establishment of testbed ● Provision of application development infrastructure (establishment of business ecosystem) ● Fostering of industry
③ International cooperation	● Collaboration with universities and research institutions ● Formation of research communities ● Formation and support for consortiums ● Organization of 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	● Development and securing of quantum natives ● Development and securing of diverse quantum human resources ● Utilization of NICT quantum security hub

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

2. Individual Promotion Strategies

(1) Research and development

【Promoting continuous R&D at NICT】
・Based on national plans and strategies as well as NICT's Fifth Medium-to-Long-Term Plan, NICT will conduct research and development of quantum network technologies and secure 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.

【Promoting technology transfer of research results at NICT】
・NICT will promote research and development for companies to catch up with the technology in cooperation with the government and other organizations. The system for transferring technologies and basic research results at NICT also needs to be improved.

06 CHAPTER.6 PROMOTION STRATEGY

【 Promoting 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 conducted mainly in Europe and the United States, it is necessary to promote R&D by establishing a system for collaboration among industry, academia, and government through national projects.

(2) Social implementation

【 Establishing a testbed 】

・ NICT will establish an open testbed that connects quantum technology innovation hubs in cooperation with the government, companies, etc., and will upgrade the Tokyo QKD Testbed. (See "Initiatives for building quantum technology platforms" on p. 61.)

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

【 Providing application development infrastructure (establishing the 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 for 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 by NICT.

(3) International cooperation

【 Collaborating with universities and research institutions 】

・ Considering international R&D trends on various quantum technologies, such as ion traps 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 repeater technology, network architecture, software, etc.

【 Forming research communities 】

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

06 CHAPTER.6
PROMOTION STRATEGY

【 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 institutes has been formed to promote quantum networks, and NICT will participate in and support such interdisciplinary communities.

【 Organizing a 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 competition and national security. NICT will also actively promote the network of global strategic partners and standardization proponents in order to build an international testbed.

【 Launching collaboration programs 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, even though the human and financial resources for R&D on quantum technology are limited.

(4) System design

【 Promoting 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).

【 Developing an evaluation and certification framework 】

• NICT, in cooperation with the government, companies, the Quantum ICT Forum, etc., will promote the development of appropriate methods for assessing the security of 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 insurance 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, which started in 2020, in collaboration with governments, universities, companies, etc. NICT will also consider developing human resources with broad knowledge including quantum algorithms, high-level programming languages, architecture, etc., as well as human resources who can design the entire system.

06 CHAPTER.6
PROMOTION STRATEGY

・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.

【Utilizing NICT's 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 the open testbed by 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 building a framework for joint use among industry, academia and government

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

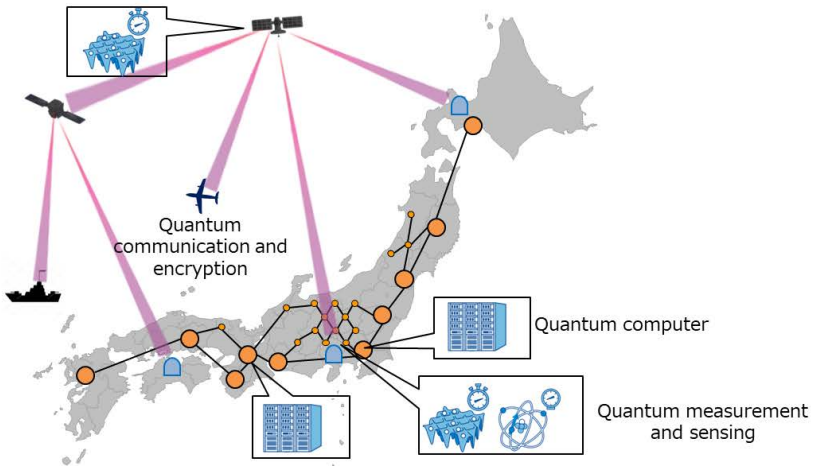


Figure 30 : Initiatives for building quantum technology platforms

07 CHAPTER.7
CONCLUSION

• This White Paper summarizes the image of society, use cases, key technologies, the R&D roadmap from 2021 to 2035, and the promotion strategy for quantum network ｓ .

• With regard to quantum networks, work on the social implementation of QKD and research and development for the Quantum Internet are under way internationally. 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 the use of quantum networks in society.

• NICT will update this White Paper based on future international trends and the latest R&D.

【 Authors at NICT 】
ASAEDA Hitoshi, ENDO Hiroyuki, FURUSAWA Kentaro, HACHISU Hidekazu, HAYASAKA Kazuhiro, IDE Shinji, IDO Tetsuya, IHARA Toshiyuki, ISHITANI Yasuki, IZUMI Akie, KANNO Atsushi, MATSUZONO Kazuhisa, MIKI Shigeto, MIYAZAWA Takaya, MOROHASHI Isao, NEMITZ Nils, OTSUBO Nozomu, SAITO Yoshihiko, SASAKI Akihiko, SASAKI Masahide, SEKINE Norihiko, SEMBA Kouichi, SHONO Shiho, TAKEOKA Masahiro, TERAI Hirotaka, TOYOSHIMA Morio, TSUJIMOTO Yoshiro, YAMAGUCHI Yuya, YANAGISAWA Kotaro, YOSHIHARA Fumiki

【 Update History 】
- Release 0.9: April 30, 2021
The English text (version 0.9) was translated from the Japanese text (version 1.0) by White Paper staff using TexTra*, a machine translation system developed by NICT.
https://mt-auto-minhon-mlt.ucri.jgn-x.jp/

Quantum Network White Paper

Published August 2021

ISBN:978-4-904020-21-0

National Institute of Information and Communications Technology

4-2-1 Nukuikitamachi, Koganei City, Tokyo 184-8795, JAPAN

E-mail nict-idi-wp@ml.nict.go.jp
URL https://www2.nict.go.jp/idi/en/