White Paper

Quantum information technology

Executive summary

The demands of 21st century information generation, transmission, and processing are rapidly exceeding the capabilities of conventional electromagnetic systems. Progress will depend increasingly on quantum information technology (QIT). This white paper addresses a wide range of considerations, from the motivations for developing QIT to the roles of standardization associated with anticipated QIT products.

There are numerous drivers for increasing investment in QIT. First, from a nation-state perspective, quantum technologies are commonly ranked with other critical research and development priorities such as artificial intelligence (AI) and biotech. Second, investments are driven by (a) foreseen domestic economic growth, (b) projected benefits of quantum computing, (c) necessity of physically secure communication protocol, (d) technological need for improved sensing devices, (e) military necessities, and (f) fear of "missing out".

The white paper introduces the current state of QIT through research and technological status, industrial status, and market status. **Quantum computing** encompasses quantum hardware, quantum error correction, quantum algorithms, and quantum software. **Quantum communication** is categorized into fibre-optic quantum key distribution (QKD) technologies, satellite-based QKD technologies, and technologies for transmission/reception elements for quantum cryptographic key distribution. Finally, **quantum sensing** includes research on quantum-based clocks, magnetic-field sensors, high-energy physics, inertial sensors, single photonic elements, and quantum imaging.

Because quantum information science and technology are still evolving, this white paper includes perspectives of both near-term potential (0-10 years), and long-term potential (>10 years).

Quantum computing research is evolving in the short term in areas including superconducting quantum computing, ion-trap quantum computing, optical quantum computing, semiconductor quantum dots systems, quantum software, and quantum simulators with some potential application areas such as deciphering, drug research and development, quantum machine learning, and search engines. However, the long-term perspective of this evolution is much more difficult to forecast.

The quantum communication research is centred on QKD technologies for the short-term and long-term perspectives.

Quantum sensing research is currently addressing the prototyping of photon sensors, atomic clocks for timing and network synchronization and devices measuring frequency spectrum, and sensing based on quantum entanglement in the short term. In the long term, large-scale quantum sensor networks will be provided, including biosensors, solid-state sensors, and atomic sensors. The forecasted availability of sensors based on quantum entanglement will provide increased performance.

The use cases for QIT encompass key technologies, state-of-the-art devices, procedures, processes, techniques, and science and standardization. Quantum computing use cases include quantum chemistry, quantum AI, quantum computing in the financial industry, quantum optimization, and quantum cloud computing. Quantum communication use cases include leased lines, virtual private networks, electric power communications, wireless communication codes,

and quantum random number generators. Finally, quantum sensing use cases include quantum acceleration sensors, quantum imaging sensors, and quantum magnetic-field sensors.

This white paper reflects current standardization activities, considerations for standardization readiness and their relations to technology readiness level (TRL), and challenges/ considerations for effective standardization. The standardization landscape makes references to key international standards developing organizations (SDOs) with a substantial QIT activity, such as ETSI, IEEE, IETF/IRTF, ISO, IEC, and ITU. Since research on QIT is still ongoing and a premature standard may include technology biases, it will be important to time the development of standards to coordinate with research status. In this context, standardization readiness takes into consideration market demand, technological and market maturity, and global expertise. Gaps in standardization are likely and these challenges illustrate the need for adequate industry engagement, creating a multi-organizational cohesive suite of standards. Finally, it must be noted that more is not necessarily better.

This white paper makes several recommendations to industry, the standardization community, and IEC standardization specifically. First, one aspect that needs to be taken into consideration is the standard readiness level of QIT. It is clear that the maturity level of QIT is different for specific technologies. Standards should be technology-neutral and therefore the standardization readiness level for each QIT area should be evaluated case by case so that standardization will not disrupt innovative progress.

From an industry perspective, this white paper recommends that industries actively engage with standardization efforts. Early engagement will provide the opportunity to align their own product development to the future standard, which will likely result in competitive advantage.

The global quantum marketplace requires a comprehensive, robust, and consistent set of standards. Therefore, proactive coordination and collaboration between standardization development and standards specification organizations will be required.

QIT standardization should be scientific-based but industry-driven, and therefore an adequate industry engagement throughout the standardization process is critical to ensure broad acceptance and buy-in from a broad stakeholder community.

Common terminology will be critical to fostering mutual understanding between the researchers and standardization experts. It is recommended that ISO/IEC JTC 1/WG 14: Quantum computing, should expand its terminology standardization effort to encompass quantum information technologies broadly. In addition, ISO/IEC JTC 1/ WG 14 should be more proactive in tracking related quantum computing standardization efforts and maintaining active relationships with other relevant standards organizations.

There is a need to develop a standardization strategy that distinguishes needs at the material, component, and systems levels. New standards efforts should be considered on a case-by-case basis, considering standardization readiness level and specific technological needs. The IEC Standardization Management Board (SMB) should initiate a discussion on the standardization strategy going forward and the division of roles and responsibilities among ISO/IEC JTC 1 and the other existing technical committees. The IEC SMB should evaluate the different standardization readiness levels (SRLs) for QIT.

Acknowledgments

This white paper has been prepared by the Quantum Information Technology project team of the IEC Market Strategy Board (MSB), with major contributions from the project partner, Korea Institute of Machinery and Materials (KIMM), Daejeon, Korea, and project leaders Dr Seong Su Park, Electronics and Telecommunications Research Institute and Dr Taik-Min Lee, Korea Institute of Machinery and Materials.

The project team was directed by Dr Dongsub Kim, Mokpo National University, Korea and an MSB member.

The project team is listed below:

Dr Seong Su Park, Electronics and Telecommunications Research Institute, Korea

Dr Taik-Min Lee, Korea Institute of Machinery and Materials

Dr Clare Allocca, National Institute of Standards and Technology, US

Dr Joonwoo Bae, Korea Advanced Institute of Science and Technology

Mr Timothy Burt, L3Harris

Dr Olaf Cames, Action-Science

Mr Takeshi Chikazawa, Mitsubishi Electric Corporation

Mr Dapeng Liu, Allibaba

Mr Daniele Dori, Tratos UK, Ltd

Mr Brian Fitzgerald, US FDA

Dr Terrill Frantz, Harrisburg University, US

Dr Barbara Goldstein, National Institute of Standards and Technology, US

Mr Yun Chao Hu, Huawei

Dr Taeho Hwang, Korea Electronics Technology Institute

Dr Munseok Jeong, Hanyang University, Korea

Dr Sohee Jeong, Sungkyunkwan University, Korea

Dr Jung Jin Ju, Electronics and Telecommunications Research Institute, Korea

Mr Nam-Joon Jung, Korea Electric Power Corporation

Mr Hyungsoo Kim, Korea Telecom

Mr Jangmyun Kim, SK

Mr Je-Hyung Kim, Ulsan National Institute of Science and Technology, Korea

Mr Seunghwan Kwak, ID Quantique

Mr Hyeokshin Kwon, Samsung

Mr Chae Lee, LX Semicon

Dr Haesong Lee, Jeonju University, Korea

Mr Gen Lei, China Electronics Standardization Institute

Mr Mengliang Li, China Electronics Standardization Institute

Mr Xiongfeng Ma, Tsinghua University, China

Mr Saejun Oh, Korea Electric Power Corporation

Mr Hee Su Park, Korea Research Institute of Standards and Science

Dr Joon-Shik Park, Korea Electronics Technology Institute

Ms Kristen Pudenz, Lockheed Martin

Mr Hai Shu, Haier Group and MSB member

Dr Jindong Song, Korea Institute of Science and Technology

Dr Edgar Sotter, CSA Group Canada

Mr Dragi Trifunovich, Mitsubishi Electric Corporation

Mr Andy Di Wang, Huawei

Dr Junchao Wang, Chinese Academy of Sciences Key Laboratory of Quantum Information

Ms Hong Yang, China Electronics Standardization Institute

Dr Chun Ju Youn, Electronics and Telecommunications Research Institute, Korea

Mr Wangtan Yuan, Haier Group

Dr Man Hong Yung, Huawei

Mr Yajun Zhang, Tencent Technology

Dr Yu Zhang, University of Science and Technology of China

Dr Li Zhengyu, Huawei

Mr Xiaobo Zhu, University of Science and Technology of China & Jinan Institute of Quantum Technology

Mr Peter J Lanctot, IEC, Project Coordinator

List of abbreviations

Technical and scientific terms

5G	5th generation
AI	artificial intelligence
APD	avalanche photodiode
ASIC	application-specific integrated circuit
BQP	bounded-error quantum polynomial time
BSM	Bell state measurement
CAGR	compound annual growth rate
CMOS	complementary metal oxide semiconductor
CV-QKD	continuous-variable quantum key distribution
DFB	distributed feedback
DI	device-independent
DV-QKD	discrete-variable quantum key distribution
EB	entanglement-based
EMS	element management system
EUV	extreme ultraviolet
FPGA	field-programmable gate array
GDP	gross domestic product
GPS	global positioning system
HAP	high-altitude platform
HEP	high-energy physics
HPC	high-performance computing
IC	integrated circuit
ICT	information and communication technology
IoT	Internet of Things
IT	information technology
ITS	information-theoretic security
LED	light-emitting diode
LiDAR	light detection and ranging

LTE	long-term evolution
MDI	measurement device-independent
MEG	magnetoencephalography
MEMS	microelectromechanical systems
ML	machine learning
MRI	magnetic resonance imaging
NGO	non-governmental organization
NISQ	noisy intermediate-scale quantum
NLP	natural language processing
NMR	nuclear magnetic resonance
NP	non-deterministic polynomial-time (hardness)
NV	nitrogen-vacancy
OEM	original equipment manufacturer
OFC	optical fibre cable
OPGW	optical fibre composite overhead ground wire
OPM	optically pumped magnetometer
OTN	optical transmission network
OTP	one-time pad
P&M	preparation and measurement
PQC	post-quantum cryptography
QAOA	quantum approximate optimization algorithm
qBLAS	quantum basic linear algebra subroutine
QCNN	quantum convolutional neural network
QEC	quantum error correction
QIaaS	quantum infrastructure as a service
QIP	quantum information processing
QIT	quantum information technology
QKD	quantum key distribution
QPaaS	quantum platform as a service
QRNG	quantum random number generator
QSaaS	quantum software as a service
R&D	research and development

RSA	Rivest-Shamir-Adleman (algorithm)
SDO	standards developing organization
Si	silicon
SNSPD	superconducting nanowire single-photon detector
SPAM	state preparation and measurement
SQL	standard quantum limit
SQUID	superconducting quantum interference device
SRL	standardization readiness level
SSPD	superconducting single-photon detector
TRL	technology readiness level
TRNG	true random number generator
VPN	virtual private network
VQE	variational quantum eigensolver

Organizations, institutions and companies

CETC	China Electronics Technology Group Corporation
ETSI	European Telecommunications Standards Institute
IBM	International Business Machines Corporation
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU's Telecommunication Standardization Sector
KIMM	Korea Institute of Machinery and Materials
MSB	Market Strategy Board (IEC)
NIST	National Institute of Standards and Technology
Q2B	Quantum Computing for Business
SMB	Standardization Management Board (IEC)

Glossary[1]

continuous-variable quantum key distribution (CV-QKD)

potentially high-performance technique for secure key distribution over limited distances

information reconciliation

technique that allows two parties knowing correlated random variables, such as a noisy version of the partner's random bit string, to agree on a shared string

Source: https://link.springer.com/article/10.1007/s001459900023

Josephson junction

quantum mechanical device which is made of two superconducting electrodes separated by a barrier (thin insulating tunnel barrier, normal metal, semiconductor, ferromagnet, etc.)

logical qubit

an abstract qubit realized by combining one or more physical qubits

physical qubit

a tangible device that implements a qubit

privacy amplification

technique that allows two parties sharing a partially secret string about which an opponent has some partial information, to distill a shorter but almost completely secret key by communicating only over an insecure channel, as long as an upper bound on the opponent's knowledge about the string is known

Source: https://link.springer.com/article/10.1007/s001459900023

quantum

minimum amount of action discretely generating multiples measurable as angular momentum

quantum algorithm

set of operations designed to run on an implementation or model of a quantum computer

quantum annealer

device that uses adiabatic time evolution to find solutions that correspond to minimum energy states

quantum communication

communication method using quantum effects for information transmission

quantum computing

information processing and entanglement engineering applying the Hilbert space formulation of quantum mechanics on different qubit modalities based on electronic, photonic, and nuclear spins

quantum correlations

the expected change in physical characteristics as one quantum system passes through an interaction site

1 Some of the definitions listed here are drawn from the latest version (under development) of ISO/IEC AWI 4879, *Information technology – Quantum computing – Terminology and vocabulary* (https://www.iso.org/standard/80432.html).

quantum cryptography

a cryptosystem based on the properties of quantum mechanics and non-classical mechanics

quantum entanglement

a property of a quantum state within a joint system of at least two Hilbert spaces that cannot be referred to as a property of its individual constituents

quantum information

the information contained in a quantum state or system

quantum key distribution

procedure or method for generating and distributing symmetrical cryptographic keys with security based on quantum information theory

quantum machine learning

machine learning making use of quantum algorithms

quantum measurement

a method to read (or probe) the state of the target quantum system

quantum sensors

according to the laws of quantum mechanics and using quantum effects, a physical device designed to perform the transformation of the measured system

quantum state

a state in the Hilbert space of a quantum system; in the context of quantum computing, often a state in the Hilbert space consisting of a tensor product of two-level systems or qubits

quantum superposition

in quantum mechanics, addition of different quantum states resulting in another valid quantum state

NOTE: Every quantum state can be represented as a sum of two or more other distinct states.

qubit

a quantum bit

NOTE: In quantum computers, information units are also called quantum bits, including “0” states, “1” states, or superposition states

Sagnac effect

a phase shift observed between two beams of light traversing the same closed path in opposite directions around a rotating object

syndrome measurement

measurement that can determine whether a qubit has been corrupted, and if so, which one

Section 1
Introduction

1.1 Background

The basic physics of conventional electronic information technologies is the science of electromagnetism, first established in the 1800s. After remarkable progress and achievements as well as contributions to industry over several decades, the physical limitations of this technology will soon be reached. There will come a time in the near future in which integrated circuits cannot be made smaller without encountering disruptive quantum effects such as tunnelling. Processor speed is also nearing the maximum possible.

At present, there are two possibilities for coping with this situation. One is to continue to optimize the usefulness and capabilities of existing technologies, improving computational disciplines such as artificial intelligence (AI) in the near term.

The other is to cross the border to the quantum world, leaving the realm of integrated circuits and exploiting the laws of quantum mechanics as first established in the early 1900s. Prototypes of quantum computing and quantum communication technologies have existed since the early 2000s. The prototypes, however, are not yet fully quantum but contain noise, and are dubbed noisy intermediate-scale quantum (NISQ) technologies. Nonetheless, quantum information technologies (QITs) will be utilized for practical application in the not-too-distant future.

This white paper aims to summarize the status of QITs. It addresses the development and evolution of quantum technologies from various viewpoints, such as a technical road map, expected applications in industry, and international standardization.

1.2 Quantum advantages

Quantum logic for information processing will lead to efficient computing, secure and efficient communication, and high-precision measurements beyond present limitations. New cryptographic systems will provide a higher level of security.

The NISQ technologies that are currently available, however, do not yet meet that level of capability. The gap between the promise of powerful quantum information processing and presently available NISQ technologies is manifest in the noise appearing in quantum systems. Error correction is therefore a key milestone on the road to progress. Nonetheless, many current quantum technologies suffice to go beyond the classical limitations and are ready to apply to computing, communication, and sensing with quantum advantages.

Understanding quantum information processing requires knowledge of, among other terms and concepts, qubits, superposition, entanglement, and unitary dynamics (see Table 1-1).

A qubit is a quantum bit, the fundamental unit of quantum information processing, analogous to the binary digit (bit) of conventional electronic computing. Qubits can be affected by superposition and entanglement, which are quantum properties that have no classical counterpart. Superposition and entanglement are important factors in quantum measurement. When identical qubits are measured in the same apparatus, they will display different properties. Quantum theory does not permit a priori prediction about specific observables but about the probabilities of measurement outcomes.

Superposition signifies the state of a qubit before a measurement such that different outcomes are possible to appear when a measurement takes place. Quantum superposition applied to computational tasks may be referred to as quantum parallelism.

Multiple qubits containing superposition may not be characterized by combining the preparation of individual qubits only. But qubits can become "entangled" such that their properties are inextricably correlated; a measurement of one will determine the properties of the other no matter how far they are physically separated.

Entanglement is a resource in quantum information processing and applied for various purposes. Because qubit information can be neither copied nor amplified, the communication distance is limited. Entanglement can be used to extend the distance. Entanglement in multipartite qubit states can realize quantum algorithms.

Quantum dynamics corresponds to a time evolution of qubits before a measurement takes place. It is characterized by a unitary transformation that is reversible unless a measurement is performed. Entanglement and superposition among qubits may be generated during quantum dynamics.

Table 1-1 | Comparison between quantum and classical systems

Properties	Comparison		Implications and applications
	Classical	Quantum	
Superposition	0's and 1's by electrical signals	0's and 1's can be superpositioned into quantum states	▪ Quantum parallelism of computing
Entanglement	Not possible	Present	▪ Long-distance quantum communications ▪ Quantum cryptography ▪ Quantum sensing
Dynamics	Irreversible	Reversible	▪ Quantum states cannot be reproduced ▪ Quantum computing

1.3 Scope

This white paper aims to cover the current status of QITs, collect activities to support their development and applications, and find expected near-term and long-term outcomes in industry.

Section 2 introduces quantum computing, quantum communications, and quantum sensing. It addresses the need for QITs and their ultimate applications. Section 3 reviews the status of current QITs from various angles: technical aspects, market status, and effect on industry. Section 4 collects near- and long-term expected outcomes. Section 5 shows applications of QITs for practical purposes. Some of the applications are discussed in terms of near-term, noisy, and intermediate quantum technologies. These include quantum machine learning, quantum communication together with smart phones, and quantum sensors. Section 6 reviews and discusses on-going standardization activities. In section 7, the white paper concludes with the list of recommendations that may maximize the usefulness of current QITs and nurture their development in a science-oriented and industry-driven manner.

Section 2

The need for quantum information technologies

2.1 QIT already offers superior solutions

The promise of quantum information technology (QIT) is not a false dawn. Impediments to the development, standardization, and commercialization that are currently regarded as hurdles will eventually be overcome through ever-growing understanding and exploitation of quantum properties.

The time will come, within the next 10-15 years, in which researchers and industry will master the quantum "ecosystem", heralding a "quantum big bang" in computing, communication, and sensing.

For perspective, it is necessary to step back and reflect on the fact that computing and sensing demands have outgrown the limits of classical physics and computing. The need for precision and fidelity of sensing is rapidly outgrowing current technology. For example, the simulation of states of a system is a highly significant benefit of QIT that meets the new needs of faster, more efficient, and more secure solutions and applications, as discussed in later sections of this white paper.

How can the case be made simply and clearly that justifies the necessity of QIT? Three factors all inextricably interlinked – are particularly relevant:

- Unmatchable speed
- Unbeatable security
- Unsurpassable scalability

This section does not aim to address each area, technology, or application where QIT is currently making an impact. Tables such as Table 2-1 have been included to list those areas that are grabbing headlines or are working quietly at the cutting edge.

This white paper also does not touch on academic research or initiatives in quantum science and technology. Although many of the next leaps in quantum knowledge-how are anticipated to take place at universities, the scope and breadth of the work undertaken in academia are beyond the purpose and space of this white paper.

- **Concept of quantum computing**

Science, medicine, finance, and communication, to name only the most visible of sectors, face seemingly endless problems awaiting substantial advances in speed, efficiency, and privacy. All confirm the need for QIT in computing, communication, and sensing, as are outlined below.

Table 2-1 | Examples of innovatione industries – comparing traditional ICT and quantum ICT

Industry	Traditional, current information and communication technology (ICT)	Quantum ICT
Artificial intelligence (AI)	Resource-hungry components (e.g. graphics processing units) and considerable time are needed for teaching AI and machine learning (ML).	AI-specific quantum algorithms enable high-speed computing. It will typically consume approximately 1/600 of power required by classical supercomputers.
Medicine/ pharmaceuticals/ chemical industries	Complex molecular structures cannot be computed virtually due to the large number of scenarios.	New computing methods optimized for the analysis of 3-dimensional structures of proteins, etc. can be utilized. Applications for discovery of new drugs, DNA analyses, development of novel matter, etc. are possible.
Finance/logistics/ vehicular traffic	Real-time analysis and application are not possible due to prohibitively large computing loads.	High-speed computing is possible by utilizing algorithms that enable real-time analysis and optimization. Can be utilized for finance (portfolio optimization), vehicular traffic (real-time traffic analysis*), etc. *Automobile manufacturers are conducting pilot operations.
Aviation/aerospace	Optimization utilizing supercomputers has limitations. Difficult to improve the performance of individual chips of supercomputers (limitation of high integration).	Quantum computers can be utilized for analyzing and understanding complex and turbulent air flow. Aerodynamic simulation of aircraft* *Undertaken by aircraft original equipment manufacturers (OEMs)

- **Concept of quantum communication**

Quantum communication involves processes in which messages are created, transmitted, and received using qubits. Quantum communications collectively refers to all the various combinations of bit and qubit data transmission/reception processes, involving multiple transmitters and receivers called "quantum network communications" (see Figure 2-1).

Quantum communication enables secure physical communication that cannot be hacked and provides transmission of quantum states between quantum devices such as quantum computers.

An illustration of the difference between traditional and quantum communication is provided in Table 2-2.

Photonic qubits are useful for transmitting quantum messages and networking distributed quantum systems. By utilizing them, distributed quantum computing networks can be created with long-distance quantum computers; at the same time, long-distance transmitters/receivers can cooperate in network coding.

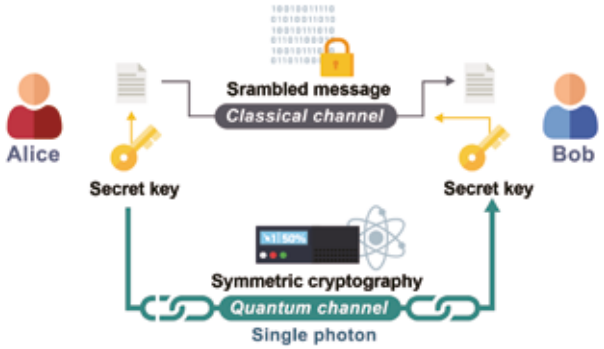

Figure 2-1 | Concept of quantum communications

Table 2-2 | Examples of quantum communication

Area	Traditional, current ICT	Quantum ICT
Communications	Potential for eavesdropping, interception, or wiretapping of terrestrial lines of communication, submarine cables, and space communication. Security issue of short-distance wireless communications such as near field communications, and of long-distance wireless communications of aircraft, diplomatic missions, etc.	Fundamental capability to prevent eavesdropping, interception, wiretapping, or hacking of terrestrial lines of communication, submarine cables, and space communication.
Distributed computing	Quantum states are converted to electrical signals for transmission (limitations of expansion).	Systems are expanded by the realization of large-scale quantum computing networks comprising small- and medium-sized quantum computers for transmitting signals in quantum states.

- **Concept of quantum sensing and metrology**

Quantum sensing is a technology that enables ultra-precision measurement by using the changes in quantum states caused by the influence of electric/magnetic fields, inertia, gravity, and photons, etc. It also includes technologies for generating and controlling single photons, single electrons, single ions, etc. to build whole quantum sensing systems.

The principle at work here is to increase measurement precision so that it is significantly higher than those of conventional sensors, by converting hyperfine wave data in quantum entangled states into measured values (see Figure 2-2). However, exploiting one single quantum of basic substance such as atomic ion, electron, photon, and so on to enhance measurement precision is still within the category of quantum sensing (atomic watch, quantum light detection and ranging (LiDAR), single-photon counter, etc.).

Readily deployable applications of traditional sensing versus quantum sensing are provided in Table 2-3, which highlights the “quantum leap” in capability that quantum sensing offers.

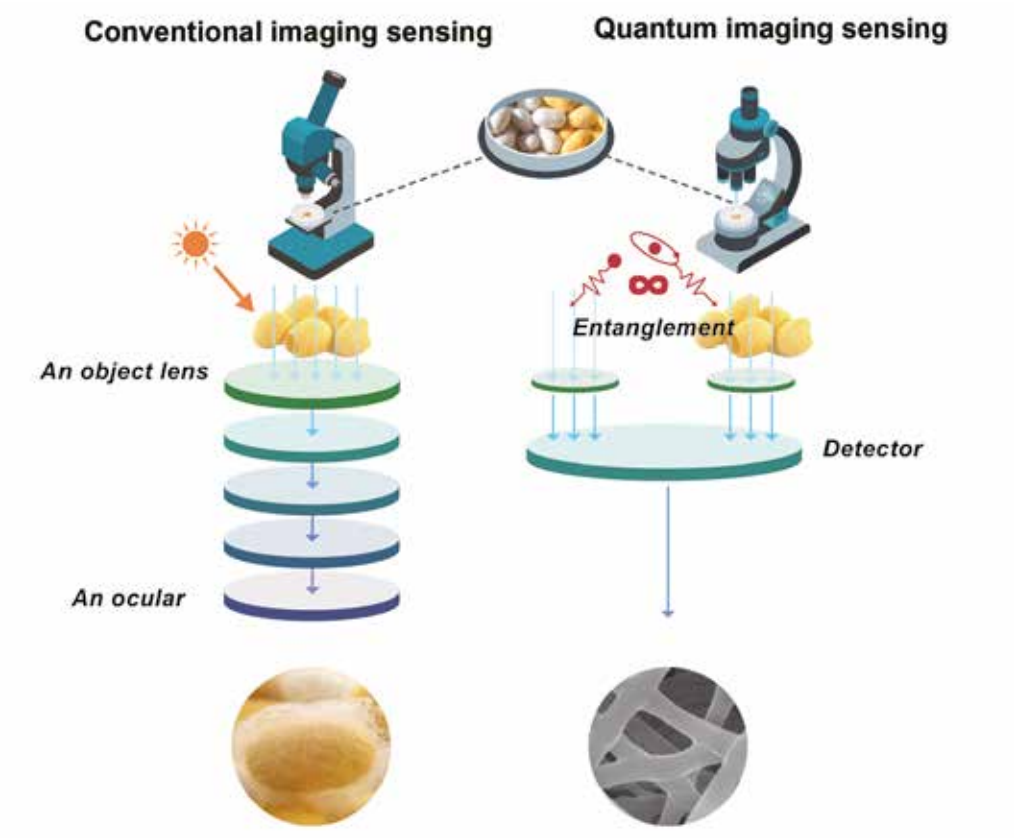

Figure 2-2 | Classical and quantum sensing

Table 2-3 | Examples of quantum sensors and metrology

Technology	Traditional, current ICT	Quantum ICT
Medical imaging	Magnetic resonance imaging (MRI) can detect cancer cells that are 5 mm or larger. Optical microscope can resolve micrometre-size objects.	Possible to detect cancer cells that are 1 mm or smaller. Quantum microscope can resolve objects around 10 nm.
LiDAR	Possible to detect objects at a distance of approximately 100 m but cannot penetrate objects.	Capable of detecting objects at a distance of 200 km or greater. Able to penetrate and detect hidden objects (stealth, blind spots). Using entangled photon pairs, it can detect stealth objects.
Underground exploration (sinkhole finder)	Can detect one five hundred-millionth of Earth's gravity.	Enables detection of at least one ten-billionth of Earth's gravity. Allows for ultra-precision detection in areas such as resource exploration, sinkholes and volcanic activity. Detection.
Global positioning system (GPS) data and inertial navigation	GPS reception error is 10 m to 50 m. Use of GPS is limited in places such as underwater areas, mines, and buildings.	Ultra-precision positioning having an error of 10 cm or less. Enables precision positioning in underwater areas, mines, and buildings (service expansion).
Lithography	Shorter wavelength is necessary for smaller integrated circuit (IC) feature size (high-cost extreme ultraviolet (EUV)).	Optical lithography around 1 nm is expected using low-cost quantum processes.

2.2 Industrial drivers of QIT

Private-sector investment shows a growing global trend, with numerous new enterprises being founded based on academic research in the areas of computing, communications, and sensing.

In addition, large multinational companies in existing legacy markets are investing in the development and commercialization of quantum technology, clearly recognizing its potential.

2.3 Potential for market growth

- **Quantum computing**

The quantum computing market – comprising hardware, software, and cloud services – is expected to increase at an average annual growth rate of 42%, reaching a market volume of USD 1,4 billion in 2027 [1][2].

It is expected that the market will grow as ICT supply networks are integrated with quantum technologies as hybrid computing frameworks are utilized, but not replacing all aspects of conventional computing. It is also expected that quantum computing will exceed the performance of conventional high-performance computing (HPC) in certain, niche computing areas and that the utilization of quantum computing will increase within the next decade.

According to industry reports on the utilizations of quantum computing by the year 2019, more than 64% of uses involved finance, energy/materials, pharmaceuticals, and medicine.

While users have great interest in these areas, experts in the relevant areas expect that the additional benefits of quantum computing can be achieved based on forecasts up to 2025 (short term) and 2035 (long term).

- **Quantum communication**

The quantum communications market, relating to quantum key distribution (QKD) devices and quantum network cryptographic services, is expected to grow at a high growth rate of 50% on average every year, reaching USD 5,5 billion in 2027 [1].

It is expected that quantum technology will be utilized in cryptographic communications and big data transmission and that these two actors will form the basis of many commercial transactions. In addition, quantum cryptography is foreseen to provide superior cryptographic and blockchain technology compared with conventional technology. Building a quantum internet is a key ambition for many countries around the world. A quantum internet would be able to transmit large volumes of data across immense distances at a rate that exceeds the speed of light [2]. This would offer solutions to the 5G technology market, which will become a core driving force of the currently growing communications market, and that quantum internet technology will provide many new applications, services, and solutions that are required by 5G technology for sensing, imaging, and positioning

- **Quantum sensing & IoT**

It is expected that the quantum sensing/measuring market will witness a growth rate of 10% on average every year, reaching USD 2 billion in 2027 [1]. The quantum technology market will be the driving force that achieves dramatically, and radically, improved sensing and measuring solutions.

An example can be seen in gravity sensors made much more precise by means of quantum sensing. Quantum electromagnetic sensing will enable the detection of minute differences in electromagnetic

2 Numbers in square brackets refer to the Bibliography at the end of this white paper.

fields, and quantum image sensing will improve spatial resolution, sensitivity, and long-distance imaging. In addition, the potential of quantum Internet of Things (IoT) will likely evolve far beyond the performance limitations of conventional IoT technology.

2.4 National investment

Nation-states in greater numbers are acknowledging a commitment to the development of quantum technology. The economically powerful nations (top-20 by GDP) are increasing their previously announced funding levels to newsworthy levels, and numerous nations in the next GDP bracket are joining in by making publicly announced investments into quantum technologies for the first time. In the global aggregate, public investment into quantum technologies is presently at an unprecedented level.

The rising and broader commitment of nations to quantum technologies can be explained by both indirect and direct factors. Indirectly, investment in quantum technology is influenced by its inclusion in the family of modern, cutting-edge electronic high technology, including AI, autonomous vehicles, and 5G, as well as other non-electronic technologies such as biofuels, pharmaceuticals/ therapeutics, and chemicals.

More directly, the present trend of increasing national investments in quantum technologies can be attributed to existing applications in metrology and sensing. Future potential uses in computing, simulation, military use, and networking are expected to drive increased investment. Also, the international race for advanced quantum capabilities and “one-upmanship” is directly fuelling investment.

Progress and competitive advantage are frequently reported – perhaps misleadingly – citing metrics such as the number of qubits in a quantum computing device, regardless of the functional quality of the said computer.

Finally, as it concerns national investment into quantum technology, other generic societal and economic factors certainly are helpful to make the case for a nation’s domestic investment into quantum technologies. It should be noted that nearly every national investment into quantum technology includes supportive language or direct funding into workforce development aspects of the quantum technology ecosystem.

There is an acute awareness that tangible benefits from investment in quantum technology will require an educated domestic workforce capable of advancing the science and engineering. This includes training a workforce that may lack advanced understand of the technology to a certain degree but can use the power the technology provides.

Section 3

Status of quantum information technologies

3.1 Quantum computing

Quantum computing is facilitated by realizing quantum dynamics – that is, transformations of a quantum state in time – for computational purposes. Just as conventional electronic computing is done on circuits composed of logical gates, transformation of a quantum state can be manipulated by a quantum circuit.

Quantum state transformations can be achieved in computationally equivalent but physically distinct ways. For example, a large-size entangled state can be exploited to transform another quantum state in a process called measurement-based quantum computing. Or quantum dynamics can be realized in continuous-time evolution, known as adiabatic quantum computing.

Current quantum technologies employ different means of realizing quantum dynamics. As yet, however, these "noisy intermediate-scale quantum" (NISQ) technologies do not permit arbitrary control of quantum states with sufficiently high precision.

3.1.1 Research and technological status

- **Quantum hardware**

The main challenge for current quantum technologies is to realize noise-free quantum hardware over which quantum algorithms can run. Depending on the types of dynamics required, e.g. circuit-based or measurement-based quantum computation, different physical systems will be required. Thus, for example, quantum circuits may be realized with trapped ions or with superconducting qubits. Measurement-based quantum computing may be realized with photonic qubits.

Superconducting quantum computer. A quantum computer can be realized with superconducting qubits, often in the form of Josephson junctions. The hardware is typically designed for processing in the radio frequency or microwave spectrum, with qubits cooled down in dilution refrigerators below 100 mK, and addressed with conventional electronic instruments. Ideally, those qubits could be integrated into a chip. This technology is of great interest to academic and governmental institutions as well as commercial sectors.

Trapped-ion quantum computing. Trapped ions can be used as qubits, with potential for use in a large-scale quantum computer. Ions can be confined and suspended in free space using electromagnetic fields. Qubits are identified by stable electronic states of each ion, and quantum information is processed through the collective quantized motion of the ions in a shared trap. Lasers are applied to induce coupling between the qubit states (for single-qubit operations) or coupling between the internal qubit states and the external motional states (for entanglement between qubits).

Quantum annealing. Quantum annealing provides a way of realizing optimal solutions by finding the lowest achievable energy states of components, or at least determining the most probable of such outcomes. As it is continuous-time evolution, it might be deemed analogue quantum computing. Quantum annealing is analogous to a process where the temperature of a physical system is raised and then lowered for

the system to converge to a stable state such as the ground state. Quantum annealers are expected to solve specific problems such as optimization problems.

- **Quantum error correction**

Quantum error correction (QEC) is used in quantum computing to protect quantum information from errors due to qubit decoherence and other quantum noise. QEC is essential to avoid or minimize noise on stored quantum information, faulty quantum gates, faulty quantum preparation, and inaccurate measurements. The primary types of QEC codes are stabilizer code and topological code.

Stabilizer codes are a general class of codes discovered by Daniel Gottesman, and by A. R. Calderbank, Eric Rains, Peter Shor, and N. J. A. Sloane [3]. These are also called additive codes.

Noise on quantum systems is due to a transition from quantum to classical states. This is referred to as decoherence. QEC provides a feasible scheme to defeat quantum noise. In doing so, quantum states are preserved and error-free for a longer time. QEC codes generally require a larger number of qubits for a syndrome measurement that tells where an error takes place. Then a correction scheme is applied.

- **Quantum algorithm**

One primary goal of quantum computing is to run quantum algorithms over quantum hardware to solve hard problems such as prime-number factoring or big-database searches. Quantum principles make it possible to achieve dramatic reductions in processing time. Quantum algorithms obtained to date can be found as applications of quantum Fourier transform or quantum amplitude amplification. The former attains an exponential speedup over its classical counterpart and can be used to realize quantum prime number factoring as well as providing quantum algorithms for solving a system of linear equations. Quantum amplitude amplification can be applied to database search and achieve a quadratic speedup compared to its classical counterpart [4] [5] [6].

Another example is Hamiltonian simulation. A quantum system of many particles is described by a Hilbert space whose dimensions are exponentially large. Simulating such a system requires exponential time on a classical computer. However, it is conceivable that a quantum system of many particles could be simulated by a quantum computer using many quantum bits similar to the number of particles in the original system. In 1996, Lloyd proposed an algorithm [7] that can efficiently simulate a class of quantum systems known as local quantum systems, extending the scope to much larger classes of quantum systems.

- **Quantum software**

Quantum software includes quantum information applications in general but also other quantum applications that take advantage of classical counterparts. The advantages include polynomial speedups, resource savings, higher levels of security, etc. In particular, quantum software has been developed by taking NISQ properties into account. Quantum software is also a useful interface between a cloud-based quantum computing service and its users. It offers a general-purpose programming language that can be used to develop quantum computing applications.

3.1.2 Industrial status

Beginning in the 2010s, global IT companies reviewed the status of computing-related future technologies, recognized the application possibilities of quantum computing, and started to make investments in research and development (R&D). Since 2016, when IBM announced a cloud service for the first time, quantum computer developments started to boom at the business level, and the boom accelerated with the launch of IBM Q Network in 2017. During the last three to five years, tens of quantum computer start-ups have been founded, and they have begun full-fledged,

competitive development of various designs for quantum computers. Initially, it was expected by many experts that quantum computers based on familiar technologies employing superconductivity and ion-trap methods would emerge into commercialization first. Many global IT companies founded R&D organizations mainly focusing on the superconductivity-based methods that are compatible with the existing semiconductor processes and have high scalability.

Still, there remain considerable challenges to achieving practical progress in higher qubit counts, longer qubit durability, and lower error rates. Quantum algorithms developed to date offer higher performance than conventional supercomputers only for specific problems. However, the performance of quantum computers has improved continuously (for example, superconductivity-based methods have improved qubit durability by 10 times every three years).

3.1.3 Market status

The quantum computing market comprising hardware, software, and cloud services is expected to proliferate to a market volume of USD 1,45 billion in 2027 (see Table 3-1). The estimate of the quantum computing market is conservative because of technical challenges that may delay dissemination of the technology. Many key technologies are still in the research stage. But it is expected that the utilization of quantum computing will grow gradually in such areas as finance, healthcare, medicine, and public sectors.

Table 3-1 | Market forecast of quantum computing (unit: USD millions) [1]

Division	2019	2020	2021	2022	2023	2024	2025	2026	2027	CAGR*
Hardware	70,8	107,4	195,4	223,0	274,7	365,6	447,7	573,2	693,5	33,0%
Software	13,2	23,9	45,0	72,2	109,4	163,9	238,0	342,8	484,0	56,9%
Cloud service	0,8	2,4	9,0	16,8	31,4	56,2	94,4	158,6	276,3	107,6%
Total	84,8	133,7	249,4	312	415,5	585,7	780,1	1 075	1 454	42,6%
CAGR = compound annual growth rate										

3.2 Quantum communication

In quantum communication, two distant parties exchange secure information by using both bits and qubits. Information prepared in qubits cannot be perfectly copied, and correlations delivered by qubits cannot be reproduced by bits. One of the advantages of establishing quantum communication by distributing qubits is the possibility of achieving information-theoretic security (ITS) without any assumptions about computational capabilities. Extensive efforts have been devoted to the implementation of QKD protocols. Recently, quantum network protocols are under investigation.

In practical implementation, photons are used as a physical realization of qubits. They can be distributed through optical fibre or in free space. Either way, a natural limitation exists in

the distance over which photons are distributed. Although quantum information prepared in photons cannot be amplified because it cannot be copied by conventional means, the limitation can be overcome by sharing entanglement with repeaters. In recent developments, satellite-based quantum-state distribution technologies can play the role of a quantum repeater.

3.2.1 Research and technological status

- **Fibre-optic quantum key distribution technologies**

QKD protocols are structured by preparation, transmission, and measurements of quantum states and photonic qubits may be transmitted through optical fibre. QKD protocols then make it possible for legitimate parties to share a secret key, a process called symmetric-key cryptography. To ensure the security of QKD protocols, it is crucial to take noise appearing in the protocol into account. For maximum security, single photons are generated. Once multiple photons are generated, they may be received by both legitimate parties and an eavesdropper who shares the same information; the protocol is no longer secure. In monitoring communications, it is assumed that an eavesdropper is present. The consequence is that an error rate may appear after measurements. Moreover, photons have a limited detection efficiency, meaning that one may fail to have a fair sample to estimate the error rate.

QKD protocols have been developed by overcoming the security loopholes mentioned above. Decoy QKD protocols close the loophole in the preparation of single-photon sources. Errors appearing in the transmission may be corrected by one-way information reconciliation and privacy amplification. Detection loopholes can be closed by measurement-device-independent QKD protocols. A device-independent protocol achieves the highest level of security without assumptions on preparation, transmission, and measurements. It is essential to distribute entangled photons in order to realize device-independent QKD protocols.

- **Satellite-based quantum key distribution technologies**

Distribution of quantum information in photons over free-space optical paths (see Figure 3-1) indicates that satellites can provide a promising avenue for a global secure quantum network.

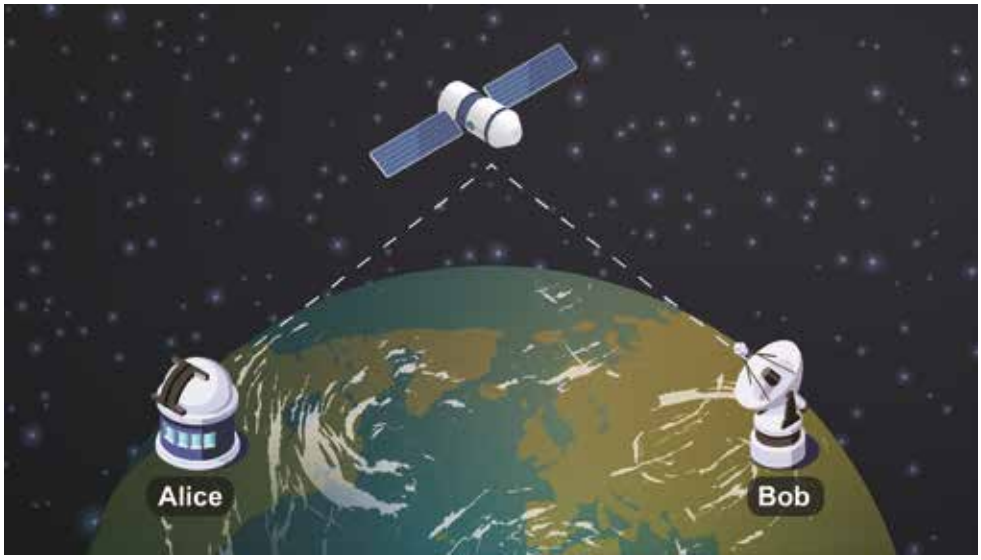

Figure 3-1 | Micius, a quantum communications satellite

- **Technologies for transmission/reception elements for quantum cryptographic key distribution**

Technologies for generating photon-based quantum signals and distributing quantum cryptographic keys are currently improving distance, speed, and integration. A compact, low-cost, and mass-producible integration technology for QKD utilizing an InP-based transmission part integration chip and a SiON-based reception part interferometer chip was developed in 2017 [8]. This technology achieved a quantum bit error rate of 1,1% and a quantum cryptographic key generation rate of 345 kbps at an optical attenuation factor of 4 dB in the BB84 quantum cryptographic protocol [9].

The possibility of a high-level QKD protocol by coupling multi-core optical cables with a QKD transmission/reception chip manufactured based on silicon photonics technology was demonstrated. Although this technology used a high-level QKD protocol and achieved a higher data efficiency than the past binary-type QKD systems, it still needs to improve the quantum bit error rate. A silicon-photonics integrated transceiver for a polarization-based QKD system was also developed in 2016. The transceiver has a subminiature transmission part in which a ring modulator, a variable optical attenuator, and a polarization modulator are integrated into the world-first integrated chip based on silicon photonics that can be utilized for polarization-encoded QKD.

A company has developed a phase-encoding QKD technology utilizing two distributed feedback (DFB) lasers [10]. This technology also employed a phase modulator using two DFB lasers based on electro-optical effects. It achieved a quantum bit error rate of 2% and a quantum key generation rate of 250 kbps through a channel of a 20 dB loss using a single-photon detector.

3.2.2 Industrial status

Quantum cryptographic protocols can be classified into preparation and measurement (P&M) methods, entanglement-based (EB) methods that utilize entangled pairs, and measurement device-independent (MDI) methods that utilize the reverse processes of entangled pair measurements (see Table 3-2).

One of the representative protocols of P&M methods is BB84. Its transmission part randomly encodes bits and bases, and its reception part randomly decodes bits and bases and uses only the bits of an identical basis as keys.

Similar to P&M methods, the EB protocol randomly modifies bases and measures entangled pairs. In this case, the measurements of entangled pairs of an identical basis show a perfect correlation, but those of different bases show unexpected results.

In MDI-QKD, the transmission and reception of secure information between two participants, Alice and Bob, encode independent qubits and send them respectively to a central third party, Charlie. Charlie carries out Bell state measurements (BSM) on the two qubits and transfers only the measurement results to Alice and Bob. In MDI-QKD, encoding quadrature such as continuous-variable QKD (CV-QKD) can be used. Because measurements are through BSM at the centre, MDI-QKD is useful in forming a star configuration network. The twin field protocol, a kind of MDI-QKD, has an extended maximum transmission range up to 404 km.

Table 3-2 | Categorization of protocols

Architecture	Protocol
Discrete-variable QKD (DV-QKD), preparation and measurement (P&M)	BB84
	B91
	COW
	T12 (modified BB84)
	DPS
DV-QKD, entanglement-based (EB)	E91
	BBM92
DV-QKD, device-independent (DI)	MDI
	Twin field
Continuous-variable QKD (CV-QKD)	GMCS (GG02)
	No-switching GMCS
	DMCS

Regarding QKD networks, although qubit states of quantum cryptograms should be transmitted end-to-end, the transmission range is about 80 km due to the transmission losses of optical cables. Unlike conventional signals, it is impossible to amplify quantum cryptographic signals due to the no-cloning rule.

At the current technology level, the transmission of quantum states is possible only at one node in QKD. Although the utilization of quantum repeaters can solve this problem, there remain technical difficulties. Therefore, in the current methods qubits are transmitted only at one node and repeated through trusted repeaters. When trusted repeaters are used, unconditional security proof is impossible. There is no adequate solution in the case of long intercontinental transmission where trusted repeaters cannot be installed. As an alternative solution, it is proposed to form quantum channels utilizing satellites. Because satellite channels have minor loss above most of the atmosphere, it is possible to transmit qubits at a range over thousands of kilometres through satellite channels.

3.2.3 Market status

The global market for quantum communications, including QKD devices and quantum network encryption services, is expected to grow at an annual average rate of 50,5% to USD 2,1 billion in 2027 from USD 80 million in 2019 (see Table 3-3). If the dissemination of quantum security devices containing quantum random-number generation chipsets increases, the quantum communications

market will grow far more rapidly. Although the growth of the industrial market has been insignificant until now, mainly involving laboratory instruments and related parts, the market will gradually expand if technologies become mature.

Table 3-3 | Market forecast of quantum communications (unit: USD millions) [11]

Division	2019	2020	2021	2022	2023	2024	2025	2026	2027	CAGR*
QKD equipment	79,34	120,2	141,3	154,2	301,0	441,7	530,1	1 118,0	1 903,0	48,8%
Quantum network encryption service	0,82	1,53	1,60	4,59	22,58	39,86	50,85	120,1	204,4	99,2%
Total	80,2	121,7	142,9	158,8	323,6	481,5	581	1 238	2 108	50,5%
CAGR = compound annual growth rate										

3.3 Quantum sensing

Quantum sensing encompasses applications of quantum systems to perform a measurement of physical quantities. Examples include atomic clocks and magnetometers based on superconducting quantum interference devices. In recent years, quantum sensing interacts with the rapid development of quantum information technologies. In particular, an entanglement that is used to achieve secure quantum communication or quantum computing is exploited in quantum metrology for an ultra-precise measurement.

On the technical side, quantum metrology with atomic qubits can be summarized as follows. First, the atoms are prepared in a well-defined state from the internal structure of atoms, e.g. a specific hyperfine state. Second, the state evolves in the presence of external interactions by which a parameter is encoded. Finally, a quantum measurement finds the encoded parameter with a high precision beyond classical limitations.

There are four necessary attributes for a quantum system to be applied as a quantum sensor [12]. First, a quantum system has discrete, resolvable energy levels that are separated by a transition energy. Second, it should be possible to initialize quantum systems in a particular state and also to read out that state. Third, the quantum system should be coherently manipulated by time-dependent fields. Fourth, a quantum system interacts with a relevant physical quantity such as an electric or magnetic field.

3.3.1 Research and technological status

For the purposes of this white paper, quantum sensing comprises methods that enable measurement of physical quantities that cannot be measured with conventional methods or measuring them at higher sensitivities [13] by utilizing quantum technology.

- **Quantum clocks**

Atomic clocks are an example of quantum technology that has been commercialized. They have become useful tools for time standardization and an international standard [14] has already been established for their use. In an atomic clock, a trapped atomic cloud is irradiated with microwaves. At one specific frequency, the atoms will resonate, absorbing and emitting photons at a maximum rate that is easily detected. Because that frequency is exactly determined by quantum physics, it serves as an ultra-accurate time standard [15], [16]. The National Institute of Standards and Technology (NIST) in the US has developed "chip-scale" atomic clocks.

- **Quantum magnetic-field sensors**

Quantum magnetic-field sensors are being utilized mainly in the areas of biomagnetic measurements such as magnetic resonance imaging (MRI) and magnetoencephalography (MEG), while R&D activities are being conducted to allow for commercialization.

MEG is a non-invasive technique to measure the tiny magnetic fields generated in the brain. Because of its excellent temporal precision and good spatial resolution of brain activity, MEG has many applications in healthcare, from clinical applications to monitor degenerative brain diseases, to neuroscience research. Conventional MEG equipment uses superconducting quantum interference devices (SQUIDs) to detect magnetic fields generated in the brain. These devices are fixed to the equipment and require a cryogenic dewar to maintain their working temperature (see Figure 3-2). This construction limits the head shapes and sizes of the subjects and requires them to be completely static during the scanning, complicating the use of this technique for children and people with illness-inducing involuntary movements such as Tourette's Syndrome or Parkinson's Disease [17].

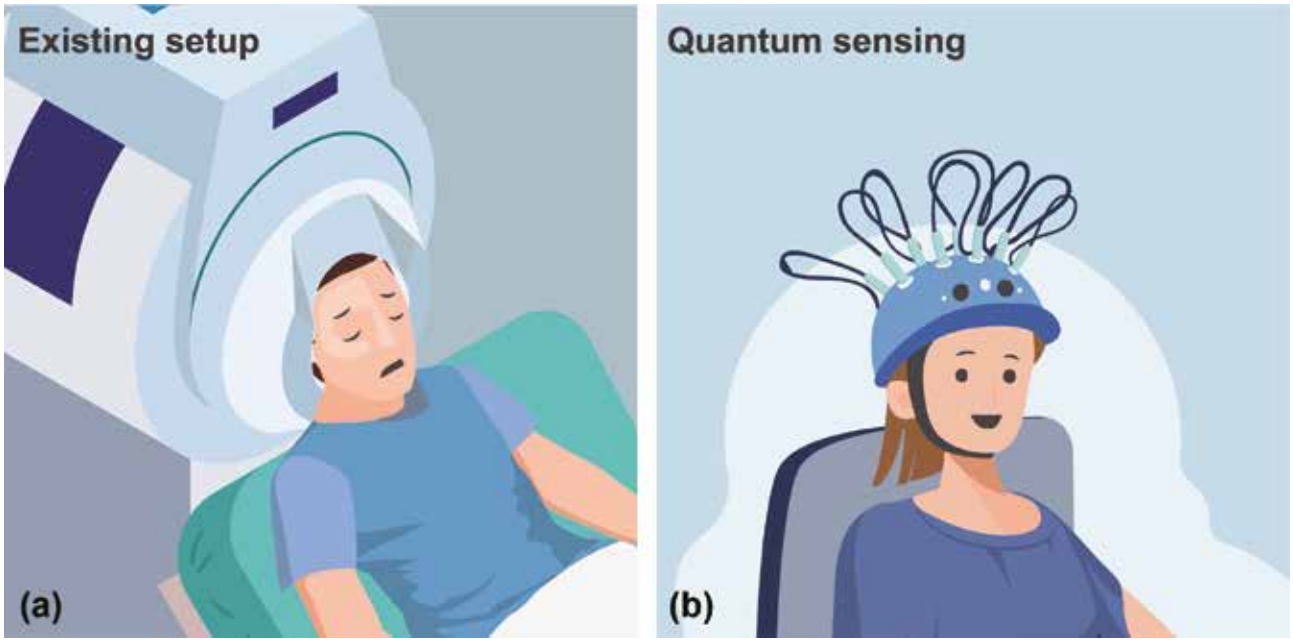

Figure 3-2 | Conventional and experimental MEG systems
(a) Conventional 275-channel cryogenic MEG system, weighing ~450 kg [18]
(b) Experimental setup of OPMs-based MEG, housed in a child's modified bike helmet

New MEG prototypes have been developed, since NIST originally patented the chip-scale magnetometer for MEG in 2004, that replace SQUIDs with quantum sensors called optically pumped magnetometers (OPMs). These sensors exploit the quantum mechanical properties of alkali atoms to measure small magnetic fields. Their sensibility is close to that of commercial SQUIDs, they can be microfabricated, and they do not require cryogenic working temperatures. The flexibility of OPMs allows the creation of wearable MEG helmets [19], reducing the cost of the equipment and opening the door to a wider set of possibilities in neuroscience research [17-20].

- **High-energy physics**

New physical particles can be detected by the tiny energy shifts they cause in quantum systems. The Heisenberg uncertainty principle limits the sensitivity of some measurements used in high-energy physics (HEP), including field measurement, position sensing, magnetometry, and interferometry. The limit placed on simultaneous measurements of two non-commuting quantities (such as the amplitude and phase, or the cosine and sine quadrature of an electromagnetic signal) is referred to as the standard quantum limit (SQL). Quantum sensors can exploit quantum correlations to make measurements beyond the SQL, improving the science reach of HEP experiments. Measurement protocols variously take advantage of squeezing, entanglement, back-action evasion, photon counting, and other techniques. [21].

- **Quantum inertial sensors**

The purpose of quantum inertial sensors is to utilize trapped ions for making precise optical measurements of variations caused by gravity or rotational inertia. Integrated research on quantum measuring theories, atomic physics, and quantum-electric mechanics of resonators is being conducted to apply noise-reduction effects based on the compression of quantum probability distributions of atomic interferometers. According to actual applications, quantum inertial sensors can be categorized as quantum gravimeters (see Figure 3-3) or gyroscopes. Gravimeters are sensitive devices for measuring variations in the Earth's gravitational field [22]. Gyroscopes are sensitive devices used to detect the deviation of an object from its initial orientation [23]. In these devices an atomic cloud measures acceleration by sensing the spatial phase shift of a laser beam along its freely falling trajectory [12].

Quantum gravimeters can spot underground structures and materials twice as deep and with higher accuracy than any conventional technology. Thus they can outperform existing methods to scan archaeological sites, explore for mineral resources, monitor volcanic activity, search for underground rock formations where CO_2 can be safely sequestered, and survey aquifers to help manage water resources [20].

Quantum gyroscopes are of great interest in the field of inertial navigation [24], a technique that continuously monitors the velocity and orientation of an object to determine its position with a reference point. This technique is very useful for applications that require precise navigation, such as autonomous mobile objects [25].

Figure 3-3 | Muquans absolute quantum gravimeter [26]

- **Single-photonic elements**

The quantum sensors applied in quantum optics are mainly based on the technology for generating single photons, and for generating/measuring entanglement of multiple photons. In order to create high-performance single-photon generators and detectors, technology utilizing diamond nitrogen-vacancy (NV) centres, superconductors, and semiconductors is being developed. Research is being conducted on how to enhance single-photon purity, photon indistinguishability, and extraction efficiency. Nano-photonics technology will support this technology.

- **Quantum imaging**

Prototypes of quantum lidars (see Figure 3-5) and radars (see Figure 3-4) that involve quantum optical sensors have been developed for capturing images. In the area of quantum microscopic technology, researchers are investigating light sources that achieve entanglement between a greater number of photons and how they can be coupled with existing microscopic structures compatible with quantum light sources. In the area of quantum polarization technology, research is being conducted on expanding the existing photonic dual light source technology for quantum entanglement between different wavelength ranges, and on improving the stability of quantum interferometers.

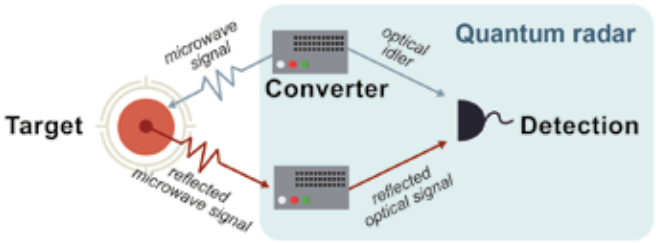

Figure 3-4 | Conceptual diagram of the quantum radar realized by CETC

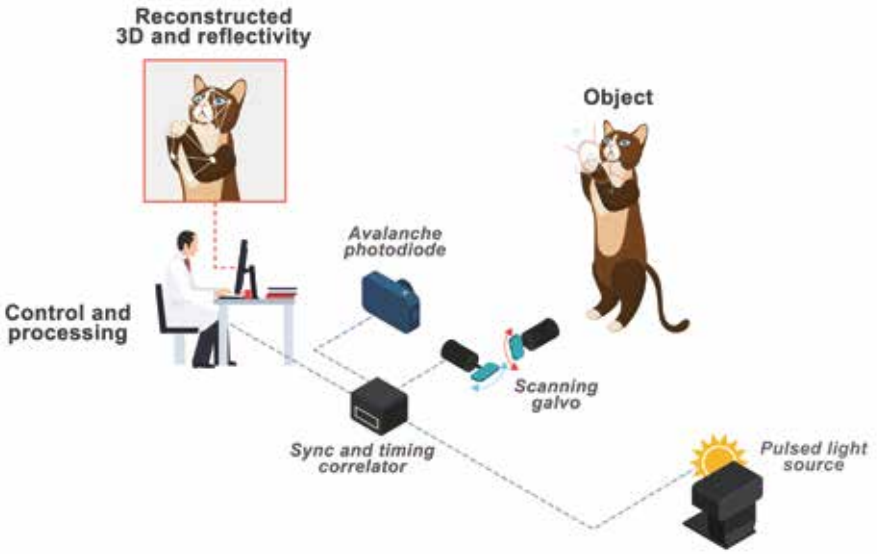

Figure 3-5 | Conceptual diagram of the quantum lidar realized by Boston University

3.3.2 Industrial status

Commercial quantum sensing technology is mainly being developed by American and European companies.

Industries, academic institutes, and research institutes (often through government-supported projects) are actively collaborating.

High-performance particle-sensing technology based on quantum optics has reached a high level of performance. Because these technologies can provide information on the movement and size distribution of particles at very high speed, they are expected to be utilized for the chemical and other related industries.

Also in development is technology that forms the basis of high-performance quantum sensors along with compact laser sources of very stable wavelengths and output power. These are essential for creating quantum imaging systems. It is expected that highly stable laser sources will be used for diamond-based quantum sensors and devices that can enable diagnosis of brain and neurological activities of patients as they undergo surgery, the detection of individual neurons, and the manufacturing of quantum microscopes for observation of live cells through low levels of medium-infrared rays [27].

Nanophotonics technology is combining with semiconductor processes for miniaturization and mass production. Also in development is a method of embedding a Si-CMOS chip for controlling the sensor.

3.3.3 Market status

It is expected that the quantum sensing market will grow at an average rate of 10,4% to USD 2 billion in 2027 from USD 0,92 billion in 2019 (see Table 3-4). Leading categories will be atomic clocks and quantum magnetic-field sensors at 30,6% and 45,7%, respectively, in 2027.

Table 3-4 | | Market forecast for quantum sensing (unit: USD millions) [28]

Division	2019	2020	2021	2022	2023	2024	2025	2026	2027	CAGR*
Atomic clock	453,0	470,1	488,1	507,1	527,3	548,7	571,5	595,6	621,3	4,0%
Gravity sensors	6,7	7,2	7,7	8,6	9,3	10,3	11,2	12,3	13,2	8,8%
Quantum magnetic sensors	408,2	450,9	498,5	551,6	611,0	577,4	751,8	835,4	929,4	10,8%
Quantum radar/lidar sensors	7,3	10,5	15,2	22,1	32,0	46,5	67,4	97,7	141,7	44,9%
Single-proton detectors	24,0	28,8	34,6	41,5	49,8	59,7	71,7	86,0	103,2	20,0%
Other quantum sensors	20,2	32,6	46,9	76,3	96,8	120,8	149,1	182,6	222,9	35,0%
Total	919	1 000	1 091	1 207	1 326	1 463	1 623	1 810	2 032	10,4%
CAGR = compound annual growth rate										

Section 4

The potential of quantum information technologies

4.1 Quantum computing

The prospect of designing and building quantum computers has justifiably received a great deal of attention in recent years. Quantum computers are devices that exploit fundamental properties of quantum mechanics to resolve specific problems that even a high-performance classical computer would otherwise find impossible to solve. If such a device could demonstrate that it can perform calculations exponentially faster than a classical computer, it would achieve what is called "quantum supremacy".

The current generation of quantum computers relies on various platforms. Those of most interest to date include ion-trap systems, optical systems, cold-atom systems, silicon systems, and superconducting systems.

In general, two types have been created so far: general-purpose quantum computers and dedicated quantum computers.

A general-purpose quantum computer utilizes quantum bits to perform expandable, fault-tolerant quantum computation, placing emphasis on the number of quantum bits and the fidelity of the logic gates.

A dedicated quantum computer exploits controlled single-body quantum systems to simulate a multi-body quantum system, resulting in vastly superior, if not unsurpassable, performance compared to classical computers. However, a dedicated quantum computer is limited to solving specific kinds of problems, and no more.

The complexity and range of unsolved challenges of practical, general-purpose quantum computers, may compel researchers to focus their efforts on dedicated quantum computers.

By numerous accounts, "quantum supremacy" [29] [30] has already been achieved by dedicated quantum computers built with superconducting and optical systems, and progress has been made in chemistry simulations [31]. Ongoing developments in quantum computing, coupled with improvements in quantum system accuracy, fidelity, and fault tolerance, strongly suggest a roadmap of quantum computing potential as outlined below.

4.1.1 Near-term potential (within 10 years)

Near-term efforts in quantum computing are anticipated to concentrate on realizing fault-tolerant quantum computation by improving the fidelity of quantum logic gates and the quantitative scale of quantum bits.

Emphasis will likely be placed on implementing fault-tolerant quantum computation culminating in general-purpose, error-correctable quantum computers that consist of hundreds of quantum bits. However, it will be problematic to achieve precise parallel control of so many qubits. Other probable impediments are programmable lattice problems and medium-scale non-lattice problems. Finally, specialized operating systems and software ecosystems will be necessary for the practical use and sustained development of quantum computers.

The performance of logical qubits is expected to be improved through repetitive error corrections of physical qubits, allowing for the development of

quantum computers of hundreds of qubits. These developments may then be deployed in the initial field tests of data centres, for example.

Eventually, beyond 10 years, quantum computing systems will comprise hundreds or even thousands of individual quantum computers (quantum simulators), making it possible to explore quantum learning theories, new algorithms, and applications, and to solve the challenges of error corrections of benchmark quantum computing simulators and existing devices. That will require an array of technologies and approaches.

- **Superconducting quantum computing**

Superconducting technologies can take advantage of advanced integrated circuit processing techniques to achieve rapid expansion in the number of qubits. However, there are shortcomings in the fidelity and coherence time of superconducting logic gates, and the difficulty of physically wiring inter-qubit connections increases significantly with greater qubit numbers.

For superconducting systems, crosstalk becomes prominent as the number of quantum bits increases. The performance of superconducting qubits is highly affected by the manufacturing process and material defects. Therefore, microfabrication techniques and top-down chip design will require further development to precisely control the parameters of greater numbers of quantum bits. In addition, with the need for superconducting quantum computers to operate at extremely low temperatures, next generation resources such as cooling systems will be needed to accommodate the thousands of quantum bits and related wiring.

Nonetheless, while it is presently very difficult to achieve global entanglement among all the physical bits, within the coming 10 years, the number of qubits will reach 1 million while the quantum volume indicators will exceed 128 [32]. The concept of quantum volume emerged a few years ago as developers and users grappled with how to evaluate the performance of the myriad quantum hardware technologies and their varying levels of operational fidelity.

- **Ion-trap quantum computing**

Ion-trap technology route has certain advantages in terms of physical bit quality and logic gate fidelity, as well as the ability to operate at room temperatures. However, the level of integration remains the biggest challenge [33], with microfabrication technology considered to be the most feasible solution.

Much work on ion-trap systems shows that motional heating limits the fidelity of quantum gates due to electrical noise. To eliminate this effect, a deeper understanding of the mechanism behind noise generation is needed, and more suitable trap materials and surface cleaning techniques need to be discovered. Future experiments will focus on enhancing the fidelity of multi-qubit quantum gates, increasing gate speed, optimizing two-dimensional ion-trap arrays, and increasing the integration level of optical and electrical control systems. [34]

Based on current progress, it can be predicted that the number of trapped-ion qubits will reach 60 in the next 10 years.

- **Optical quantum computing**

Optical quantum technology represents advantages in coherence time, room temperature operation, high-dimensional entanglement manipulation, etc., and has natural advantages in the realization of quantum information system interconnection. However, a complete architecture of the quantum computer still needs to be developed and hard bounds on the required performance of photonic components need to be studied. High-brightness single-photon sources, entangled photon sources, and detectors need further development. To achieve error correction, it is also necessary to study how to effectively control many error-correcting quantum circuits on the nanosecond time scale.

The current pace of R&D suggests that the number of optical qubits will reach 200 within 10 years [32], a stage at which currently unsolvable problems will be successfully tackled, and the milestone of "quantum supremacy" will have been achieved.

- **Semiconductor quantum dots systems**

A major focus in the near term will be on high-fidelity two-qubit gates. Problems such as the construction of two-dimensional array structures, the practical architecture of high-density wiring in low-temperature environments, and the establishment of precisely positioned donor arrays will likely be solved.

- **Quantum software**

Quantum software will provide applications and advanced tools that can improve performance of quantum computers and processors, demonstrate improved fault resistance, and make it possible for alternative computing models for developing architectures to be pursued. In order to construct a large-scale quantum computing cloud based on processors of several qubits, basic distributed quantum computing techniques will need to be tested with results applied to selecting future platforms.

- **Quantum simulators**

Through the precise preparation, manipulation, and detection of a large-scale multi-body quantum system, a quantum simulator capable of coherently manipulating hundreds of quantum bits is anticipated within the ten-year horizon, with such simulators able to solve a number of problems of great practical value in fields such as quantum chemistry, new material design, and optimization algorithms.

Various quantum algorithms, such as prime factorization and search algorithms – for which quantum computers are well suited – will, without a doubt, foster more application-specific dedicated quantum computers for fields such as those discussed below in the rest of this subsection.

- **Deciphering**

Most current cryptosystems are based on RSA public key algorithms whose security is guaranteed by the difficulty of completing prime factorization in polynomial time using classical computers. However, Shor's algorithm [35] has shown that it is able to break RSA cryptosystems in polynomial time using fault-tolerant quantum computers, suggesting that today's cryptosystems need to be re-examined.

- **Pharmaceuticals and therapeutics R&D**

In designing a novel drug, computer simulations are needed to find the most effective molecular structure, and the resources required for the simulation grow exponentially with the increasing number of molecules and atoms. Quantum computers represent a formidable tool to conduct large-scale chemical simulations for the development of novel drugs and therapeutics.

- **Quantum machine learning**

Machine learning is widely used in many fields such as data analysis, pattern recognition, and bioinformatics [36].

- **Search engines**

Grover's algorithm [37] has demonstrated the capability of effectively accelerating a search of large datasets.

4.1.2 Long-term potential (beyond 10 years)

In the long term, more quantum algorithms and applications will continue to emerge. Quantum computers will play an essential role in more fields, such as big data operations, AI, and biochemistry. The commercialization of cloud-based quantum computation is gradually maturing and will accelerate.

The use of quantum computers for solving complex computing problems will become the norm and the combined application of classical computers and

quantum computers will become the mainstream computing method in the future.

User-friendly quantum computers of hundreds of qubits, which data-centre personnel can efficiently operate, will be ready to be developed based on fault resistance realized by technically relevant algorithms within scalable architectures. Quantum simulators will be utilized for solving problems relating to materials science that supercomputers cannot solve, and non-lattice problems requiring 100 or more individual quantum systems will be simulated. Quantum simulators will be utilized for optimizing applications not only in physics but also in new areas such as AI.

A brief outline of the potential for quantum computing beyond 10 years includes the following:

- **Superconducting quantum computing**

The number of qubits in a single system are estimated to reach 2 000 000, while the quantum volume indicators will exceed 1 000 [38].

- **Ion-trap quantum computing**

The number of qubits will reach 100.

- **Optical quantum computing**

The number of qubits will reach 300.

- **Quantum simulators**

Improvements in the control precision of qubits will demand new levels of tolerance thresholds (>99,9%), millions of qubits, realization of fault-tolerant quantum logic gates, and programmable general quantum computing prototypes.

4.2 Quantum communication

4.2.1 Near-term potential (within 10 years)

Technologies for autonomous QKD systems for metropolitan [36] and urban areas are expected to achieve low-cost, high-security key rates of 10 Mbps or faster, including multiplexing (Stage 4 technology readiness level (TRL)). Systems for certification and standardization of quantum communications devices will likely be established according to the requirements of the security community, industries, European Space Agency, and government authorities (Stage 7 TRL).

Methods for realizing QKD devices can overcome the limitations of direct-wired communications, utilizing high-altitude platforms (HAPs), satellite-integrated trusted nodes, and quantum repeaters [38] (Stage 4 TRL).

The performance of multi-party network building blocks based on quantum repeaters and quantum entanglement [39] will be improved (Stage 4 TRL) through the development of core technologies such as efficient and scalable interfacing with quantum memories, frequency modulation, teleportation, entanglement purification, error correction, single photons, and entangled light sources.

Also on the horizon are practical protocols and various types of efficient algorithms for quantum networks, such as digital signatures, location-based verification, security sharing, and anonymous data queries (Stage 6 TRL).

Demonstrations will be carried out for: long-distance transmission through target tasks for supporting QKD on test bed networks, trusted nodes, HAPs, and satellites (Stage 7 TRL); realization of multi-nodal or inter-city network switches linked with components of infrastructure (Stage 7 TRL); automated, autonomous QKD systems suitable for low-cost mass production (Stage 7 TRL); realization of QKD systems of 100 Mbps or faster that improve secure key rates on urban streets (Stage 5 TRL); and networks based on quantum repeaters and quantum entanglement beyond the ranges of direct communications (Stage 4 TRL).

Along with the prerequisite of visible and demonstrable security, hardware and software developments, including device-independent protocols for realizing quantum entangled networks, will be made (Stage 5 TRL).

4.2.2 Long-term potential (beyond 10 years)

The ultimate goal is to realize the generalized use of autonomous QKD systems and networks [40], device-independent quantum random number generator (QRNG) systems and QKD communications for urban streets (Stage 7 TRL), and quantum cryptography over a range of 1 000 km (Stage 7 TRL).

To ensure the success of all these objectives there is a hard requirement for dedicated engineering support from the broadest spectrum of R&D. Engineering as well as control solutions will enable scaling of volume manufacturing – e.g. development of high-speed electronics and optoelectronics, including field-programmable gate array/application-specific integrated circuit (FPGA/ASIC), integrated photonics, packaging, compact cryosystems, and other key enabling technologies – to provide solutions compatible with operating in existing communication networks.

Progress will require establishing theory and software development of protocols and applications that build on, or go beyond, standard QKD-based basics. Critical advances will include novel approaches for system certification, including methods to test and assess the performance of quantum networks, more efficient algorithms, and security proofs targeting practical systems, including the combination of classical and quantum encryption techniques for holistic security solutions.

Transmission distance and key/data rates are the primary metrics to evaluate progress for quantum internets [41]. Increasing transmission distance will be critical to expanding the utility of QKD to more applications, and additional, higher key rates will be required depending on the quantum communications application. QKD can tolerate relatively slower key exchange rates on the order of a few keys per second, whereas distributed quantum computing and quantum sensor applications would require far faster rates. Cost is another key metric as current QKD system costs are currently prohibitively high for many applications.

Commercialization of quantum repeaters represents an important technological milestone and may enable revolutionary progress in quantum communications, including remote sensing and distributed quantum computing. Various physical approaches are also being pursued to develop a quantum repeater [42], [43]; however, it is anticipated that it will take longer than the next 10 years for quantum repeaters to be commercialized. Interestingly, the further development of satellite-based QKD represents a very feasible, alternative approach to increasing transmission distance, but data rates need to improve further. Incremental improvements may come from improved components such as lower-loss fibre optics and lower-noise, higher-efficiency, faster detectors, as well as higher-quality quantum light sources.

4.3 Quantum sensing

4.3.1 Near-term potential (within 10 years)

Quantum sensing technology not only ultimately supports the advancement of quantum computing and quantum communication technologies, but also enables a number of cutting-edge R&D projects.

Technologies that target Stage 5 TRL comprise a very broad range of developments in improved measuring and instrumentation including: electric current, resistance, voltage, photon, and electric/magnetic fields; chemistry and materials analyses; medical diagnoses based on molecular-level nuclear magnetic resonance (NMR); labelling; trace-element detection; prototyping of compact integrated photon sensors with a continuous train of single photons that can capture enhanced images at low illumination; enhanced resolution or detection of longer/hidden images of objects or specular gases; development of sensors that can

detect gravity, gravity variation, and acceleration for civil engineering and navigation purposes; and the development of miniature atomic clocks for timing and network synchronization.

Further development will include devices for processing radio frequencies, microwaves, and optical signals in managing frequency spectra for communications applications, as well as development of optical/microwave sensing and imaging technology based on quantum entanglement that can be used in ultra-high-resolution microscopes for capturing images at much lower exposures than existing microscopes or detecting stealth objects that will not let the reflected signal return.

The development of other applicable technology will, in the meantime, aim for lower TRLs of experimental concept validation based on quantum methodology such as optimized squeezed states. Naturally, well-developed sensor networks, solid-state IC chips, and Si-photonics with integrated optics will support the real application, miniaturization, and convergence of quantum sensors.

4.3.2 Long-term potential (beyond 10 years)

Although projecting developments beyond 10 years may appear to be speculation, the quantum IT community is, even at this stage, able to conceive of what lies beyond.

Better-performing index monitoring is forecast to be realized through commercial sensors and infrastructure such as frequency transmission networks and large-scale sensor networks (Stage 9 TRL, demonstrated in operational environments) and commercial bio-sensors and general-purpose electric quantum standards developed based on solid-state and atomic sensors (Stage 9 TRL). Sensors based on quantum entanglement, which have higher performance than the highest-level devices based on independent quantum systems, are also on the horizon (Stage 7 TRL).

Miniaturized quantum acceleration sensors will develop further, based on Si semiconductor processes and nanophotonics – fields that are already advanced.

Quantum gravimeters will also be actively used in exploring underground resources, detecting sinkholes, and monitoring volcanic activity and earthquake precursors caused by magma movement. These same quantum gravimeters may also find use in small drones, autonomous vehicles, and even orbital satellite groups for full and real-time monitoring of the globe.

Further down the road, quantum compasses may be employed for navigation systems in autonomous vehicles, drones, underwater drones, etc. These devices will be utilized as the main sensor for small-sized drones in exploring underground tunnels and caves and conducting search and rescue activities aboveground such as in building collapses, or in locating lost hikers and mountain climbers or even lost pets.

Even further into the future, quantum imaging sensors will find application in quantum lidars with only a single-photon generator and single-photon sensor to realize long-distance imaging, likely generating images at a faster rate. This same device will not only acquire long-distance images but also be capable of tracking a flow of gas at a long distance. Additionally, quantum imaging sensors are likely to become tools for evacuating people in the case of a fire or effluence of toxic gas, or even be part of a basket of technologies that will be able to remotely, reliably, and quickly, predict the collapse of a dam, bank, or building.

Precise quantum microscopes already developed for chemical engineering and biotechnology with quantum imaging sensors will evolve to support imaging at even faster rates and with a wider spectrum of wavelengths by creating light sources and sensors, sharing fundamental principles

with quantum lithography systems. Accordingly, semiconductor features on the order of 10 nm or less may be possible without extreme ultraviolet (EUV) lithography. Of course, EUV lithography could support a narrower process, while the semiconductor process could possibly replace, at low cost, small-dimension operations now performed with EUV lithography.

Beyond the 10-year horizon, it seems reasonable to assume that quantum magnetic resonance imaging (MRI) will first appear as a quantum magnetic sensor. The idea behind a quantum MRI – which images at the quantum level using electron spins – is to do the same for chemical reactions including those involving metal ions[3]. While existing SQUID-based magnetometers require cryogenic cooling and take up large amounts of space, quantum MRI could function at room temperatures in extremely small dimensions. Thus, affordable quantum MRI, rather than high-performance quantum MRI, would replace existing MRI devices to offer affordable MRI scanning. High-performance quantum MRI would also be expected to detect microcarcinoma at an early stage, analyze the deterioration of a battery, and detect semiconductor device defects, among other applications.

3 https://doi.org/10.1038/nature.2017.21573

Section 5

Use cases for quantum information technologies

5.1 Quantum computing

Development of industrial quantum computing applications has begun. In the next five years or so, quantum computing based on noisy intermediate-scale quantum (NISQ) [44] technologies are expected to make breakthroughs in computational science. Some probable outcomes are listed below.

5.1.1 Quantum chemistry

- **Description**

Quantum chemistry [45] is one of the most promising quantum simulation applications, aiming to uncover the secrets of electronic structure and molecular dynamics. Simulation and analysis of chemical reaction processes are extremely challenging for a classical computer because of the complexity of variables and the difficulty of modelling, and the computational burden will grow exponentially. Quantum chemical simulation has broad applications potential in the R&D of chemical agents and biomedicine and will become one of the potential markets for quantum computing. Quantum simulation can improve drug discovery rates and save development time, while better molecular design can improve drug approval rates. Several quantum cloud computing companies have cooperated with pharmaceutical companies to carry out application exploration and research.

- **State of the art**

In the meeting named Q2B (Quantum Computing for Business) in December 2017, the term NISQ was coined for the characterization of state-of-the-art quantum technologies. Hardware for quantum computing will be eventually error-free. Until then, the number of qubits tends to be large, but noise is present everywhere from preparation to measurement readout. Noise that leads quantum to classical transitions has a profound effect on quantum hardware. For example, qubit information may be affected by very small changes in ambient temperatures or electromagnetic fields.

In the next 5-10 years or so, the importance of NISQ technologies will increase.

The advantage of NISQ technologies is that the working principles are quantum; the disadvantage is that noise exists everywhere. The challenge for NISQ applications is how the quantum principles can be exploited to gain quantum advantages in the presence of noise. At the same time, NISQ technologies should provide a guide for the next step toward error-free quantum computing. This may include the realization of quantum error-correcting codes, or significant improvement on quantum hardware technologies where errors may be sufficiently suppressed.

- **Key technologies**

NISQ technologies at present have limited capabilities. For instance, quantum circuits fitted with NISQ technologies are short in depth, such that universal quantum computing that achieves an arbitrary transformation of quantum states cannot be realized. Quantum software in the NISQ era should be devised by taking the limited capabilities into account.

A well-known instance of quantum software fitted with NISQ technologies is a variational quantum

algorithm, also called the hybrid quantum-classical algorithm, that repeatedly utilizes short-depth quantum circuits (see Figure 5-1). As the hardware technologies such as superconducting qubits are developed, the variational quantum algorithms may be extended in a wide range of applications.

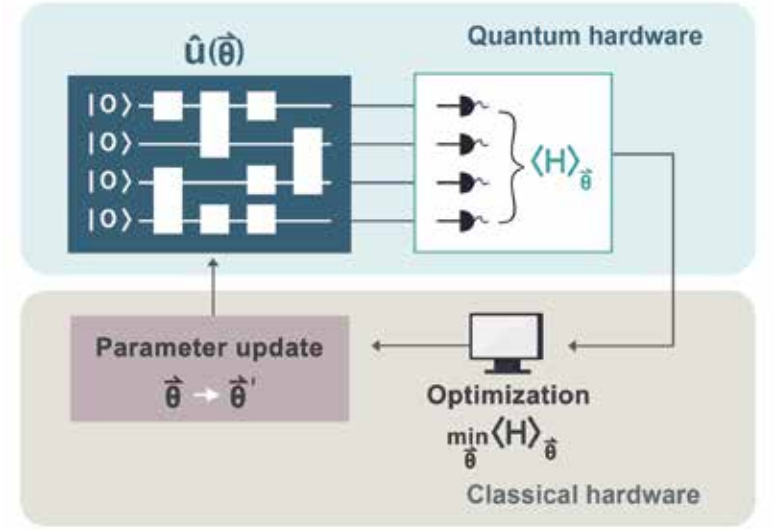

Figure 5-1 | Architecture of the variational quantum eigensolver

The quantum part in variational quantum algorithms is composed of state preparation and a measurement readout, where the outcomes can estimate the desired quantity such as energy. The classical part updates the parameters so that state preparation is optimized. In doing so, a variational quantum algorithm is dealing with an optimization task beyond the limitations of conventional classical computation.

Variational quantum algorithms processed in the presence of noise may be improved by quantum error mitigation techniques that aim to maximally suppress the effect of noise. Gate-error mitigation deals with noise appearing in a quantum circuit. Measurement-error mitigation reduces the errors in state preparation and measurement (SPAM).

Variational quantum algorithms have crucial limitations. The first is that a variational quantum algorithm strongly depends on the state preparation, called the ansatz construction, in fact, an ansatz is sometimes thought of as a "trial answer" and an important technique in solving differential equations (Gershenfeld). The second is a barren plateau that naturally occurs when random quantum gates are repeatedly applied and averaged, leading to exponentially vanishing gradients in parameterized quantum circuits.

5.1.2 Quantum AI (machine learning)

- **Description**

Quantum information techniques can also be applied to AI. Global IT enterprises are paying attention to quantum computing with the expectation that successful realization of quantum computing will result in practical use of quantum-based machine learning (ML) and AI. In the case of algorithms that fall under bounded-error quantum polynomial time (BQP) among the core elements of ML and AI, it is expected that quantum computing

will solve problems more straightforwardly and efficiently over classical computing. BQP can be viewed as the languages associated with certain bounded-error uniform families of quantum circuits (Gershenfeld).

- **State of the art**

Currently, quantum AI investigates how results and techniques from quantum computing can be applied to AI, and vice versa. The fact that quantum computing exploits exponentially large dimensions may open new opportunities to enhance AI algorithms. Conversely, AI algorithms may suggest new types of quantum software that can be realized in a quantum computer. The way quantum algorithms are designed according to the laws of quantum mechanics inspires heuristic approaches in AI.

- **Key technologies**

– Quantum-enhanced machine learning

Quantum computing can perform parallel information processing and can execute faster quantum search algorithms, which promises significant enhancement to ML where large data sets are utilized.

Quantum basic linear algebra subroutines (qBLAS) – Fourier transforms, finding eigenvectors and eigenvalues, solving linear equations – exhibit exponential quantum speedups over the best classical counterparts. This translates into increases in processing speed for many ML algorithms, including linear algebra, clustering, least-squares fitting, gradient descent for a linear system, Newton's method, principal component analysis, Boltzmann machines, feature extraction, recommendation system, support vector machines, and more [46].

Furthermore, quantum computers could narrow down the range of possible input variables and solutions to a problem that classical computers cannot efficiently obtain. It is reasonable to postulate that quantum computers will be able to recognize some particular patterns more efficiently and outperform classical computers on some ML tasks.

– Quantum-applied machine learning

Quantum-applied ML is about utilizing ML as a key tool to help improve problem-solving in quantum information processing (QIP). In the last few years, ML has exhibited significant effectiveness on QIP problems: quantum signal processing, quantum metrology, Hamiltonian estimation, quantum control, and quantum circuit compilation.

– Quantum-generalized machine learning

The majority of ML literature deals with classical data. By contrast, quantum-generalized ML processes fundamentally quantum data. As in quantum supervised and unsupervised learning, the data points are now actual quantum states.

Recently Cong et al. [47] propose a quantum convolutional neural network (QCNN) by a quantum circuit generalized from the classical convolutional and pooling layers, suitable for learning quantum states.

– Quantum-inspired machine learning

Quantum-inspired ML means applying the methods utilized in quantum physics to classical ML. Prominent new research is employing tensor networks in place of neural networks for learning architecture [46]. Moreover, a tensor product composition model (the CSC[4] model) has been introduced in natural language processing (NLP) to incorporate grammatical structure into algorithms computing meanings [47].

4 The CSC acronym is based on the initial letters of the three authors who introduced it: Coecke, Sadrzadeh and Clark.

5.1.3 Quantum computing in the financial industry

- **Description**

Among the various use cases of quantum computing, the financial industry [48] can benefit more from NISQ quantum computers, if only in sampling and in reaching decisions on a response to customers. For example, wrongful uses of credit cards amount to several tens of US billion dollars each year, and wrong management (errors in credit analysis) of customer data in financial loans causes heavy damage to financial institutions. Because the volumes of financial markets have already reached USD 2 trillion in exchanged traded fund markets and USD 3,5 trillion in asset management markets, it is expected that financial institutions will see a benefit of at least USD 10 billion through risk management of relevant assets.

- **State of the art**

In analyses of customers' credit utilizing quantum optimization algorithms, the higher the number of variables and data to be considered, the more the difficulty increases exponentially, such as in the case of non-deterministic polynomial-time (NP)-hard problems. Therefore, the current limitations of the increase in qubit counts should be overcome.

- **Key technologies**

Problems such as price-setting of financial derivatives, the credit rating of individuals/companies, and valuation of insurance products occur on vast scales. Simple stock transactions entail relatively easy problems of optimization because they involve only tens of thousands of items at the most. But the problems of assessing insurance, credit, and derivative products require significantly larger scales of optimization, because it is necessary to assume probability distributions of tens of millions of individuals (or a large number of insurance products contracted with them) and millions of enterprises and to consider their correlations. Because demands for evaluation solutions based on quantum computing are significant in terms of practical applications as well as academic research, quantum computing needs to achieve higher performance than classical computing.

5.1.4 Quantum optimization (process optimization, network optimization, etc.)

- **Description**

Optimization problems [49] involve finding the optimal solution from many possible solutions. For traditional calculations, in complex systems such as large-scale logistics networks, designing optimal routes that meet various needs requires many calculations. For example, for a logistics network with hundreds of distribution centres, it would take billions of years for traditional computers to analyze all possibilities. Quantum computing can significantly improve computing efficiency, thereby improving operational efficiency and reducing carbon emissions in logistics and transportation, air travel, traffic control, financial asset management, and network infrastructure. Current and future industries applicable to or affected by quantum optimization, such as network communication, financial analysis, and transportation planning are all based on operations research, especially the combinatorial optimization problem.

- **State of the art**

The combinatorial optimization problem refers to finding the optimal (or suboptimal) solution in a limited set of feasible solutions. It has a wide range of applications in the industrial world, such as route planning and network traffic distribution. Finding a way to speed up the solution of such problems will make it possible to significantly reduce production costs and improve many aspects of human society. As the scale increases, computational complexity makes it difficult for classical computers to solve combinatorial optimization problems with limited time and computing resources. With the help of the natural advantages of quantum computing for

NISQ devices, the quantum annealing algorithm, and quantum approximate optimization algorithm [49] proposed by industry are expected to reduce the difficulty of solving these problems. [50]

- **Key technologies**

In addition to the applications mentioned above, hybrid-based algorithms such as quantum approximate optimization algorithms (QAOAs) [49] can be utilized (see Figure 5-2). In particular, because theories are being presented that efficient combinational optimization calculations are possible even in the case of quantum annealers such as produced by D-Wave Systems, which are categorized as being of sub-compatibility with quantum computers, it is expected that the realization of more platform types can increase the feasibility.

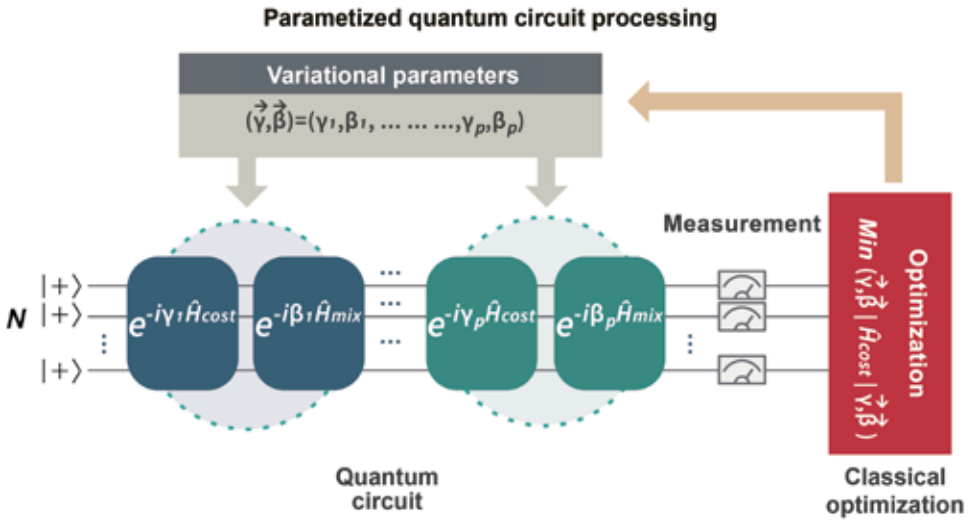

Figure 5-2 | Schematic of a p-level QAOA

5.1.5 Quantum cloud computing

- **Description**

A cloud-based quantum computing service [51] develops interfaces between users and a quantum computer (see Figure 5-3). Prototype quantum computers based on NISQ technologies are available from industry vendors. They are realized on various platforms such as superconducting qubits, photons, and ions. In cloud-based quantum computing, a user sends a design of quantum circuits or a sequence of instructions. After the request is run, measurement outcomes affected by noise are returned to the user. Since the quantum computers provided by industry vendors have not yet reached universal applicability, they may be problem-specific (e.g. optimization problems).

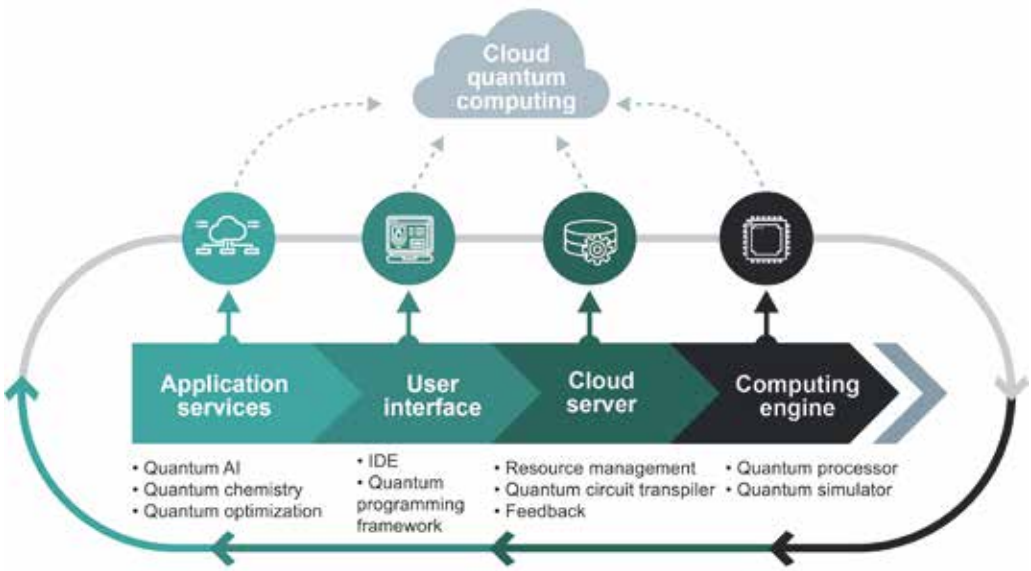

Figure 5-3 | Quantum computing cloud architecture

- **State of the art**

Quantum processors not only serve as the core "engine" of quantum cloud computing (see Figure 5-3), but are also necessary for the implementation of quantum cloud computing back-end. At present, research in quantum computing physics platforms is moving towards a breakthrough in logical qubits. Research no longer simply pursues the number of qubits but also pays attention to the simultaneous improvement in the quality of logic gate fidelity and coherence time. The most important thing needed is efficient software to control the quantum chip.

At present, quantum computing software is still in the early stage of development. Since the implementation logic of quantum computing is different from classical computing, classical computing software cannot be fully transplanted to quantum operations. Systems and application service software need to be rebuilt under the framework of quantum cloud computing.

- **Key technologies**

Although limited by existing technology, quantum cloud computing services may become the optimal solution for the general public to be able to access and use quantum computing. The architecture of quantum cloud computing should be flexible and scalable. The top-down architecture for quantum cloud computing should include quantum application services, quantum compilers, quantum code, quantum measure and control systems, quantum chips, and/or quantum simulators on high-performance supercomputers.

Quantum infrastructure as a service (QIaaS) provides basic computing and storage resources, such as quantum computing schedulers, simulators, and devices. With the development of physical platforms and technology, the number of QIaaS models providing computing engines will increase, and the computing types of QIaaS will be enriched due to diversity of quantum computing hardware technology in the future. Real quantum devices can also be divided into universal quantum processors and quantum annealing machines. Currently, many international cloud computing industries are active in QIaaS and promote the development of new supercomputing services.

Quantum platform as a service (QPaaS) provides a software development environment for quantum computing and quantum ML algorithms, a quantum programming framework, and a quantum algorithm library, and allocates hardware server computing resources over a cloud server layer connection. The QPaaS model provides services to connect other companies' hardware resources and supports cross-platform compatible development without requiring users to learn multiple development environments. It lowers the barriers to entry for software users and application developers. It also supports the debugging, diagnosis, and optimization of quantum lines through simulators, as well as automatic allocation of resources required for classical computing and quantum computing optimized hybrid quantum algorithms, and fully managed operations to increase efficiency and reduce costs.

Quantum software as a service (QSaaS) provides packaged application services such as data analytics tools, material design (e.g. quantum chemical simulation), and services such as pharmaceuticals, smart cities, and AI-accelerated computing, based on specific industry scenarios and application requirements. Today, as quantum cloud ecosystems mature, the number of QSaaS model start-ups offering solutions to specific problems is increasing. With the further development of the quantum computing industry and the gradual opening up of quantum cloud ecology, more vertical enterprises will try to develop their business capabilities through the QSaaS model.

5.2 Quantum communication

Quantum communication established by exchanging qubits involves an important property: qubit states cannot be copied. It naturally follows that quantum communication can solve the key distribution problem in a symmetric cryptosystem, QKD, the first application in quantum communication. The security of a cryptographic system is identified by a secret key (see Figure 5-4). QKD aims to provide secret keys by distributing qubits. QKD contains information-theoretic security (ITS) and relies on laws of quantum mechanics without additional assumptions such as computational capabilities.

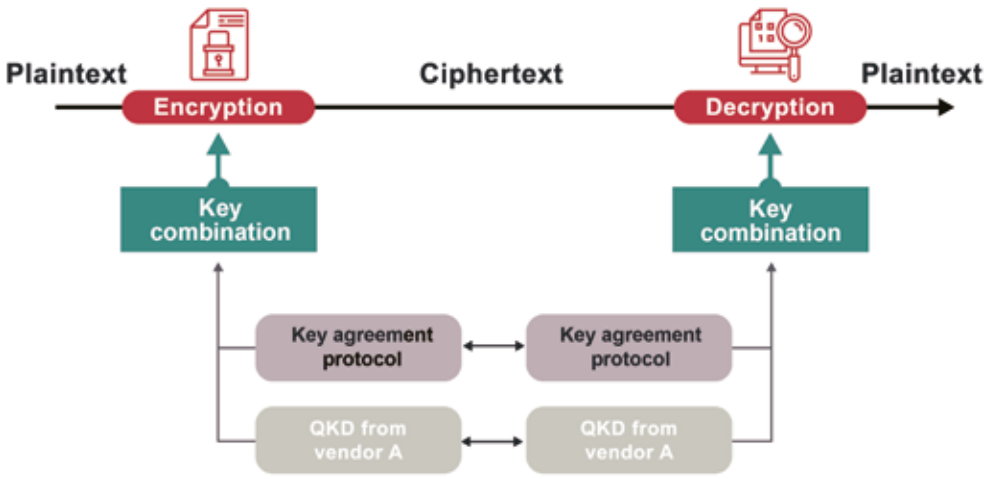

Figure 5-4 | Combination of QKD with key agreement protocol

5.2.1 Leased lines

- **Description**

Because leased lines [52] are provided for communications of enterprises and government agencies, they should be safeguarded against illegal eavesdropping or hacking. Hacking threats can be prevented by applying quantum cryptographic keys created by QKD devices.

- **State of the art**

Increasing connectivity by applying quantum cryptographic functions involves additional costs. The construction of QKD devices requires additional optical cables for quantum channels and connectivity for synchronization among QKD devices and data exchange channels. Resources can be wasted due to a lack of suitable quantum cryptographic transmission network structures. Whether dealing with customer-side transmission devices comprising a small number of lines of specific capacities or with large-scale transmission devices comprising multiple lines of various capacities, it is necessary to provide adequate QKD devices and quantum cryptographic devices for each leased line. Early dissemination of QKD devices is constrained because QKD device manufacturers utilize proprietary types and technologies. QKD devices should be embedded in transmission devices and made interoperable with quantum cryptographic devices.

- **Key technologies**

It is necessary to minimize the cost of additional connectivity in applying quantum cryptographic functions. For example, such cost can be minimized by making a single optical cable accommodate quantum communications, data, and service channels by separating them according to wavelengths. In addition, it is necessary to obtain the flexibility of QKD and quantum cryptographic devices. For example, functions such as the store and forward function and the mixed keys function can be utilized in developing various models of devices or key management devices. In designing, constructing, and operating optical communications transmission networks, there must be adequate structures to accommodate quantum cryptographic devices or to develop quantum cryptographic devices independent from transmission devices.

5.2.2 Virtual private networks

- **Description**

Virtual private networks (VPNs), which are communications networks providing security among far-off locations, have the merit of saving communications costs of leased lines, which are mainly used for internal data communications of enterprises. In particular, it is urgent to improve the security of VPNs against hacking trials because VPNs are being utilized as a communications infrastructure for teleworking, which has recently increased due to the outbreak of the COVID-19 pandemic.

- **State of the art**

Network operators will need to develop and restructure interfaces for QKD devices of cryptographic modules because VPN devices (firewalls, routers, and switches) have their cryptographic functions (cryptographic modules). Increasing connectivity for applying quantum cryptographic functions involves additional costs. The construction of QKD devices requires additional optical cables for quantum channels. In addition, it requires connectivity for the synchronization among QKD devices and for data exchange channels.

- **Key technologies**

It is necessary to develop and establish international standards for pursuing interoperability because interfacing between VPN devices and QKD devices can be hindered by proprietary technologies or dissimilar designs of device manufacturers. It is necessary to minimize the cost of additional connectivity for applying quantum

cryptographic functions. For example, such cost can be minimized by making a single optical cable accommodate quantum communications, data, and service channels by separating them according to wavelengths.

5.2.3 Electric power communications (utilities)

- **Description**

Because electric power data are of great national importance, they are generally managed through dedicated communications networks. It is expected that more and more various devices will be connected to electric power networks. More electric power data are transmitted/received through communications networks along with the recent adoption of intelligent electric power networks, the expansion of distributed electric power sources, and the developing trends of IoT technologies. Therefore, quantum cryptographic communications should be applied to improve the protection level.

In particular, in cases where optical fibre composite overhead ground wires (OPGWs) [53] are installed at the upper stream of power transmission lines for communications networks, quantum cryptographic communications can be constrained by environmental factors [54], [55]. It is essential to consider developing technologies for overcoming such constraints.

- **State of the art**

Because OPGWs are installed outdoors on electric power transmission towers, external environmental factors such as temperature changes and wind-generated vibration are likely to affect OPGW-based communications' reliability negatively. In addition, because an extension of communications lines requires physical jointing at the intervals of approximately 3 km, communications losses will inevitably occur. At each distance of approximately 40 km, the communications loss of OPGWs is about 19 dB, significantly higher than the 9 dB loss of the general communications based on optical fibre cables (OFCs).

While there are few use cases of OPGW-based quantum cryptographic communications, the demand for developing technologies for long-distance communications is increasing. Therefore, it is necessary to construct demonstration testbeds for conducting continual research.

- **Key technologies**

It is necessary to analyze constraints in the range of OPGW-based quantum cryptographic communications. In addition, it is necessary to do research on how to analyze the reliability of OPGW-based quantum cryptographic communications, which is different from that of the general OFC-based communications, and how to minimize constraints in the communications range.

It is also necessary to standardize device development and associated technologies for coping with environmental factors of long-distance transmission and optical communications lines that affect the generation of quantum cryptographic keys and the transmission of encrypted data.

5.2.4 Wireless communication code

- **Description**

Along with enhancing personal authentication and work processing based on wireless networks [56] and devices such as smartphones, it is necessary to reinforce their security when structured in interconnection with the lines dedicated to optical networks

- **State of the art**

For applying quantum cryptography, additional costs will occur because separate dark fibres should be installed and because fixed channels should be obtained for processing signals in synchronization with quantum channels and post-processing, as well as application of quantum

cryptography to existing optical transmission devices. In the case of distances beyond the typical distance limit of each node of quantum cryptographic transmission, extension solutions will be required, and the nodes should be expanded through trusted repeaters.

- **Key technologies**

It is necessary to apply cryptography to the output sections of existing optical transmission devices that receive quantum keys. The burden of cost and operation of commercial long-term evolution (LTE) networks should be minimized by applying compatible quantum cryptography. Operational risks should be minimized by a redundant configuration of dark fibre (fixed channels for synchronization with quantum channel and post-processing) and devices. Concurrent operation should be made at a distance of 36 km and at 50 km. It should be possible for a control centre to monitor the conditions of QKD devices in real time through element management system (EMS) [57] functions. It is necessary to maintain the devices of the existing optical transmission networks (OTNs) and optimize the quantum cryptographic devices' compatibility with the OTN devices. Applying EMS to the centralized control of QKD devices should be possible to monitor and respond to errors.

5.2.5 Quantum random number generators

- **Description**

The level of randomness in random number generators is one of the crucial elements in the security of cryptographic algorithms. Quantum random number generators (QRNGs) [58] produce a sequence of random numbers where the randomness relies on the laws of quantum mechanics. QRNGs are a key component in prepare-and-measure QKD protocols and can also be used in modern cryptographic protocols to improve security. Random numbers have various industrial applications, including simulations and numerical optimization in which QRNGs can be utilized to improve the level of randomness.

- **State of the art**

The existing random-number sequences needed for an authentication have been based on generation algorithms or the use of specific physical random numbers. However, such random numbers can be hacked, and their patterns can be predicted. While QRNGs can solve these problems and provide genuinely random numbers stably, they involve additional QRNG chips and costs. While authentication algorithms of the classical methods require continual random numbers, algorithm-based random numbers can form patterns due to low entropy. Several hacking cases have been reported relating to some hardware-based true random number generators (TRNGs), which are much affected by ambient environments. Because QRNGs generate random numbers by utilizing the quantum randomness that occurs when quantum states do not match their measuring bases, they can generate random numbers at higher stability and entropy. A QRNG chip was applied to a 5G smartphone in 2020 for the first time. The QRNG chip, approximately 2,5 mm by 2,5 mm, generates quantum random numbers by a method in which a complementary metal oxide semiconductor (CMOS) sensor receives photons emitted by a light-emitting diode (LED) light source.

- **Key technologies**

QRNGs should be designed to consume minimal power and their physical dimensions should be minimized so that they can be mounted in smartphones. The stability of their random number generation should be verified. It is also necessary to develop interfaces for applying QRNGs to the existing systems.

5.2.6 Post quantum cryptography

- **Description**

Once a key is established by QKD, it is then used for secure communication via classical encryption algorithms. To realize information-theoretic security (ITS) in this encrypted communication, it is essential to combine QKD with an ITS encryption algorithm such as a one-time pad (OTP). However, due to the speed limitation of current QKD systems, it is now customary to combine QKD with non-ITS cryptographic [59] algorithms, whose security relies on unproven conjectures called computational assumptions.

In near future, quantum computers may be able to break encryption algorithms currently used. Therefore, it is necessary to develop post-quantum cryptography (PQC) which is secure against cryptanalysis by using quantum computers.

- **State of the art**

Many crypto researchers are studying PQC, especially hash-based signatures, lattice-based cryptography, code-based cryptography, multivariable cryptography, and isogeny-based cryptography.

- **Key technologies**

Current concerns about deploying PQC against classical schemes include the processing speed, the size of hardware and/or software, and memory problems. It is expected to develop PQC with high processing speed and small size of hardware and/or software.

- **Standardization**

PQC is researched and studied by some SDOs/organizations:

– NIST: Post-Quantum Cryptography Project [60].

– ETSI: Quantum-Safe Cryptography Working Group [61].

– CRYPTREC [62]: Technical Report on Post-Quantum Cryptography [63]

– ISO/IEC JTC 1/SC 27/WG 2: Standing Document on Post-Quantum Cryptography.

ISO/IEC JTC 1/SC 27/WG 2 develops and maintains the standards related to cryptography and security mechanisms. It has decided not to standardize PQC at this moment because it is too early to do so, but it produced the standing document on PQC to prepare the standardization in near future.

ISO/IEC JTC 1/SC 27/WG 2 SD8, Post-Quantum Cryptography [64], consists of six parts:

– Part 1: General

– Part 2: Hash-based signatures

– Part 3: Lattice-based mechanisms

– Part 4: Code-based cryptography

– Part 5: Multivariate cryptography

– Part 6: Isogeny-based cryptography

Several algorithms/mechanisms are described in each part.

5.3 Quantum sensing

5.3.1 Quantum acceleration sensors

- **Description**

A quantum inertial sensor [65], [66] provides an optically precise measure of displacement caused by gravity or rotational inertia. An integrated study has been conducted on the quantum measurement theory, atomic physics, and resonator quantum electrodynamics technology to apply an effect to reduce noise by the compression of a quantum probability distribution. As such, quantum inertial sensors could be classified, depending on their actual application, into quantum gravitational sensors and quantum compass (quantum angular acceleration sensor).

- **State of the art**

A study has been conducted on quantum gravitational sensors and related devices to commercialize sensors that detect utility-pipe conduits and effects of natural disasters, such as volcano eruption. However, most quantum gravitational sensors are still in the prototype stage. For instance, a quantum gravimeter prototype developed has been employed in detecting activity in the Mt. Etna volcano (Italy). It is 10 times more precise and 100 times smaller than conventional gravimeters. But such a prototype is subject to environmental constraints such as extremely low temperature, large volume, etc.

As an alternative to existing quantum gravitational sensors with a long free-fall distance, a method that will make it possible to measure gravitational changes over several micrometres using an optical lattice is under development. To improve portability dramatically, developing new low-temperature atom control technology is required through interdisciplinary cooperation among atomic physics, photonics, materials, and microelectromechanical systems (MEMS). This sensor exhibits performance exceeding the sensitivity and absolute accuracy of the corner tube (FG-5) that is the existing gravitational standard. Moreover, it displays the fastest measurement repetition rate among sensors providing an absolute gravity value.

A quantum/angular acceleration sensor is referred to as a compass. Because it is basically a type of quantum inertial sensor, it shares its core technology with quantum gravitational sensors. To improve mobility and environmental sensitivity, research has been conducted on the source technology to couple micro atomic beam platforms with photonic crystals/MEMS and secure a highly integrated laser system. This technology is expected to be used in the future to track a position when moving underground or underwater, where it is hard to use GPS.

Prototypes have been produced to commercialize quantum compasses whose positional precision is 500 times better than the existing inertial sensors based on the Sagnac effect.

- **Key technologies**

A nanocrystal technology based on a silicon semiconductor process will be coupled with a silicon photonics technology for miniaturization, mass production, and entanglement of photons. Most sensors operate at low temperatures. Thus, developing new materials that allow operation at room temperature will be required. Commercialization of quantum inertial sensors will require a method to mass-produce gas cells and a method to reduce power consumption.

5.3.2 Quantum imaging sensors

- **Description**

Ultra-precision quantum imaging/polarization sensors are needed to meet demand. It is necessary to develop quantum sensing systems as national strategic technologies for national defence and facilities security and to improve spectrometric resolution and efficiency by enhancing existing imaging sensors and spectrometers.

- **State of the art**

One candidate system implemented as a single-photon light source with semiconductor quantum dot technology was based on the Purcell-enhanced micropillar system [67]. It achieved the following: single-photon purity of 99,1%, photon indistinguishability of 98,5%, and extraction efficiency of 66%. In a separate project, researchers generated a single photon with a wavelength of 1 550 nm and an entangled quantum light with indium arsenide/indium phosphide (InAs/InP) semiconductor quantum dot. Other researchers developed a highly efficient technology to couple quantum structure, and a silicon-based optical chip that could generate a single photon in optical communication wavelength band was developed.

Yet another researcher developed a technology to produce an optical fibre-integrated element by precisely recoupling a semiconductor quantum dot and optical fibre through technologies to preliminarily measure the position of the quantum dot and control the position of optical fibres. With this, it is possible to remove optical loss in an external optical system by directly coupling the optical fibre system with a single-photon source without using bulk optical components such as a lens.

A superconducting single-photon detector (SSPD) [68] based on conductivity transitions in nanoscale superconducting wires was introduced to detect a single photon without gating electronic elements because of its low dark current. It is suitable for a QKD system and processing of different quantum data. In another experiment, a single-photon detector was implemented that could perform free running with GHz frequency gating based on indium gallium arsenide/indium phosphide (InGaAs/InP) semiconductors and negative feedback avalanche.

Research has been conducted on miniaturizing quantum optical sensing elements with existing silicon photonics. This technology could arrange light sources and light-receiving elements to have high optical coupling efficiency. Recently, researchers devised for the first time an on-chip quantum element that couples a diamond ring-type resonator, including nitrogen-vacancy (NV) centre and nano-optical waveguide.

Another researcher developed a prototype that produced an image of an object 45 km away with quantum sensors [69]. In 2021, he announced a quantum sensor that could acquire an image at an ultra distance (up to 200 km), which existing sensors could not measure, and a means of seeing an object behind a wall. It was reported that a quantum radar could detect an object at a place 100 km away based on a single photon detector and the researchers declared that they validated its performance experimentally.

At the other end of the dimensional scale, quantum microscope technology has focused on light sources that implement entanglement among numerous photons, and research is underway to couple quantum light sources with the existing compatible microscopic structure (see Figure 5-5). In 2021, a researcher reported a feasible quantum microscope.

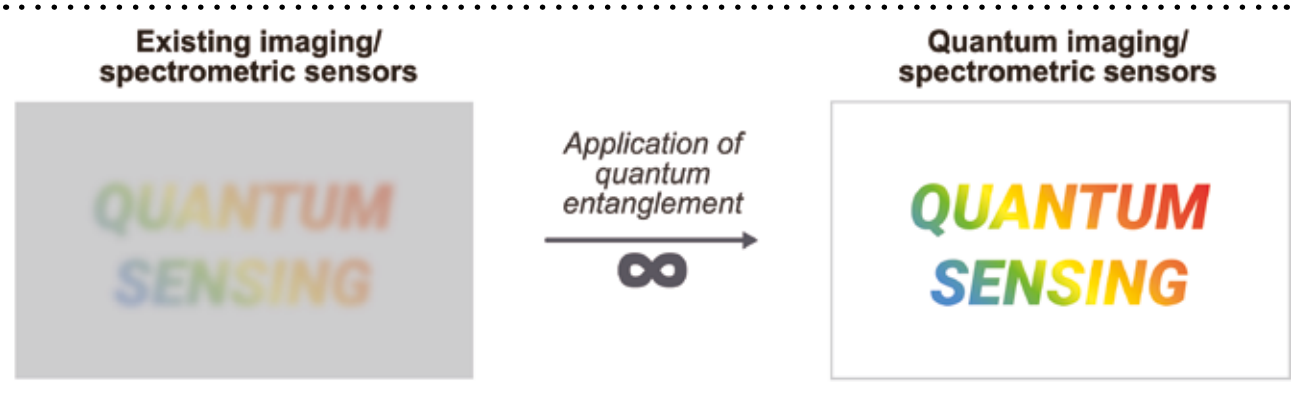

Figure 5-5 | Quantum imaging

- **Key technologies**

Progress in quantum imaging sensors will require imaging technologies for utilizing quantum entangled light sources, technologies for certifying and assessing image improvements, image processing programmes for lidars, and technologies for realizing high-efficiency single-photon detectors and photon-RF entanglement technology (radar systems). In addition, development of quantum spectrometric sensors requires technologies for dual-photon light sources, interference technologies for utilizing dual-photon light sources, quantum spectrometric technologies for medium-wave infrared rays, and technologies for high-efficiency visible-ray spectrometry. Continuous and fast generation of identical single-photon trains will be required, as will coupling of a photon with other qubits such as trapped ion, and enlargement of wavelength selection for single photons.

5.3.3 Quantum magnetic field sensors

- **Description**

Demand for high-sensitivity bio-imaging technologies is increasing in such areas as precision diagnoses of brain damages, cardiovascular diseases, and other conditions affecting the growing elderly population. In addition, the importance of infinitesimal chemical analyses is growing to reduce the time for new medicine development and for early detection of harmful factors (such as viruses). Furthermore, along with the developments in industries involved in brain-computer interfacing, demands are increasing for compact wearable biomagnetic sensors of high reliability.

- **State of the art**

Quantum magnetic field sensors can be used in biofeedback measurement, such as magnetic resonance imaging and magnetoencephalography, and R&D have been conducted for its commercialization. A magnetoencephalogram sensor is being evolved into a wearable device through miniaturization, and an atom steam cell platform is being mainly used. Researchers are conducting basic research on technologies to examine stem cells at the atomic level. Some atom stem cells were used to obtain the minute biomagnetic field distribution on a cellular level. An imaging method that employs detection of spin from diamond colour method that uses spin with a focus on diamond colour has arisen over the last 10 years [70]. Nanocrystalline diamond is harmless to humans and may be used as a contrast medium to improve the resolution of MRI images.

- **Key technologies**

Core technologies should be developed for high-sensitivity magnetoencephalographic sensors, including those for superconductivity/atomic-cell-based magnetic field sensors having sensitivity at the level of picotesla or smaller, for wearable measuring systems based on the arrangement of array sensors, and for wearable systems based on miniaturized magnetoencephalographic sensors. For magnetic field imaging based on diamond colour centres, it is necessary to develop technologies for generating colour centres at nanometre-level depths below surfaces, controlling their quantum states, and developing magnetic-field imaging sensors that can detect single cells at spatial resolutions at the level of micrometres or smaller. In addition, for developing magnetic resonance technologies based on diamond colour sensors, it is necessary to develop technologies for nano-diamond contrast media that can improve MRI resolution through high-efficiency spin polarization.

Section 6

Standardization landscape for quantum information technologies

6.1 Current standardization activities in quantum information technologies

Standards, whether in the form of physical references, software, or documents, form an invisible matrix of elements that underpin the global marketplace and provide a basis for innovation. When developed through a transparent and inclusive process, founded upon sound science and aligned with industry needs, standards can capture best practices and represent the "distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent – people such as manufacturers, sellers, buyers, customers, trade associations, users or regulators" [71]. They can open markets and democratize innovation by clearly defining device interfaces, leaving companies to then focus on how their offerings add value rather than how they will interconnect in a multi-vendor environment. Standards can encourage technology adoption by providing consumer confidence in the safety and efficacy of products.

While most of the quantum technologies being developed are still early on the technology readiness scale, the industry has begun to consider future standardization needs in the pursuit of a robust global marketplace. Several international standards developing organizations (SDOs) are facilitating the development of standards and related documents, and have already released publications, many of which are directed towards the more mature sub-topic of QKD. There is also significant work progressing in terminology and the extension of current classical standards to accommodate quantum-based technologies, and some exploratory work is being done on architectures for future quantum networks.

Table 6-1 provides a summary of current directions in quantum standardization being pursued by major SDOs. It reflects progress toward voluntary consensus-based documentary standards and does not reflect work on physical standards represented by reference materials or measurement services.

Table 6-1 | Current standardization activities

Description of SDO quantum-related activity	Selected deliverable topics	Type of output (e.g. report, interoperability standard, test protocol, procurement specification, etc.)
The **European Telecommunications Standards Institute (ETSI)** is the EU's recognized regional standards body for telecommunications, broadcasting, and other electronic communications networks and services. Relevant work takes place in the Technical Committee on Cyber Security (CYBER) and the Industry Specification Group on Quantum Key Distribution for Users.	QKD: authentication, components & internal interfaces, architectures & frameworks, vocabulary, case studies, optical characterization Quantum computing impact of ICT systems Quantum-safe cryptography: security, schema, assurance	Informative: group reports, technical reports, white papers, ETSI Guides Normative: technical specifications, group specifications
The **Institute of Electrical and Electronics Engineers (IEEE)** is a US-based professional association that has established thousands of standards for consumer electronics, computers, and telecommunications. IEEE Quantum is an IEEE Future Directions initiative launched in 2019 that serves as IEEE's leading community for all projects and activities on quantum technologies and has developed a project plan to address the current landscape of quantum technologies, identify challenges and opportunities, leverage and collaborate with existing initiatives, engage the quantum community at large, and sustain the US federal Quantum Initiative in the long-term.	Software-defined quantum communication Quantum technologies definitions Quantum computing performance metrics & performance benchmarking	Normative: standards

The **Internet Research Task Force (IRTF)** focuses on longer-term research issues related to the Internet while a parallel organization, the **Internet Engineering Task Force (IETF)**, focuses on shorter-term issues of engineering and standards making. The Quantum Internet Research Group is addressing the design and build of quantum networks. Issues to be explored include routing, resource allocation, connection establishment, interoperability, and security. This group will also perform coordination with other SDOs.	Applications, use cases & architectural principles for quantum internet Transition from classical to post-quantum cryptography	Informative: informational documents Proposed standards
The **International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)** Joint Technical Committee (JTC) 1 has two entities currently developing quantum technology standards. Most efforts will be from Working Group (WG) 14 Quantum computing, while Subcommittee (SC) 27 Information security is specifically addressing QKD security and PQC.	Terminology Security requirements, test and evaluation methods for quantum key distribution Post-quantum cryptography	Informative: standing document Normative: international standards
The study groups (SG) of the **International Telecommunication Union's (ITU) Telecommunication Standardization Sector (ITU-T)** assemble global experts to develop international standards known as ITU-T Recommendations. SG 13 Future Networks, SG 15 Transport, Access and Home, and SG 17 Security are in the process of developing documents of interest to quantum technologies.	QKD networks – security, management, architecture	Recommendations Normative: international standards

6.2 Standardization readiness

It is not easy to determine when a technology area is ready for standardization, and more specifically which kind of standard(s) would support and advance an emerging marketplace. At the highest level, there are a number of major elements that need to be in place before pursuing standards development:

- **Market needs**, evidenced by the existence of commercial products or prototypes from multiple global parties;
- **Global expertise** that is available and willing to work together to develop standards; and
- **Consensus among multiple global stakeholders**, e.g. industry, consumer associations, academia, NGOs, governments.

Once these factors are met, there are many other considerations, such as:

- **Technological maturity**. Has the underlying science been well-proven? Does sufficient measurement science exist to create a basis for a standard? Have performance expectations been set and accepted globally?
- **Market maturity**. Are there commercial products available? Does their production or use rely on a network of suppliers? Are they intended to interoperate?
- **Level of risk** the industry is willing to embrace. Will the technology and thus the standards evolve quickly, or is the industrial climate cautious and risk-averse?
- **Regulatory needs**. Will regulations incorporate standards for the industry? If yes, will these standards be voluntary and consensus-based? While regulations might incorporate standards, global standards do not address regulation. Regardless, the global marketplace will be more efficient and standards will be most useful if they do not conflict with anticipated regulations.
- **Existing standards**. Are there consensus specifications being broadly adopted as de facto standards? Should any of these be incorporated into documentary standards? Are there existing standards that can be extended to meet the needs of emerging technologies?
- **Political climate**. Are there political pressures that may influence the timing or engagement in standardization activities?

Different kinds of standards are needed to support the maturation of emerging technologies. Standards should be based on well-proven science and address commercial needs. Defining standards too early can lock in immature or inferior technologies or give specific companies or countries an unfair market advantage. Table 6-2 suggests what kinds of standards should be considered at different levels of technology maturity:

Table 6-2 | Standardization readiness

Stage of technology development	Technology readiness level (TRL)	Standardization activities to consider beginning	QIT item
Basic research	1. Basic principles observed 2. Concept/ application formulated	Identify critical measurements needed	Quantum error correction, quantum certification
Feasibility research ▪ Multiple independent research groups	3. Proof of concept	Terminology standards Test and measurement standards	Elementary quantum gates
Prototype development ▪ Commercial R&D being performed	4. Component/ subsystem validation in lab setting 5. Component/ subsystem validation in relevant environment	Characterization and performance standards Metrics and benchmarks	Integration of quantum gates, quantum certification Superconducting nanowire single-photon detectors (SNSPDs) and In(Ga)As avalanche photodiodes (APDs) of long-wavelength single photon detectors for quantum imaging sensors High-speed entangled photon generators for quantum imaging sensors
Product development Multiple companies	6. System/sub-system prototype demonstration in a relevant environment 7. System demonstration in relevant environment	Interface standards	Cloud quantum computing Trapped-ion chamber and gas cells for quantum acceleration sensors High-quality lasers and optical parts for quantum acceleration sensors Diamond NV-centres for quantum MRI Single-photon generators for quantum imaging sensors Cost-effective entangled photon generators for quantum imaging sensors

Commercial products offered by multiple companies	8. System completed and qualified through test and demonstration 9. System proven through successful operation under expected operating conditions	Testbeds Certification standards Procurement standards	Circuit-based quantum computers (IBMQ, IonQ, Rigetti), Adiabatic Quantum Computers (D-Wave) Si-based APDs for quantum image sensors Electrical communication methods to atomic clock

6.3 Standardization challenges

Effective standards:

- are science-based
- are industry-driven
- are developed by consensus among experts
- don't lock in proprietary technologies, pick winners and losers, or stifle innovation
- contribute to an open, plug & play international market
- evolve as technologies emerge and mature
- are broadly adopted

It is beneficial to standardize quantum sensing according to the core parts of each application. In other words, the application can be divided into quantum gravity sensor, quantum compass, quantum MRI, quantum lidar, etc., but the standard is to exchange atomic ion cells, diamond defect-based quantum magnetic sensor parts, single-photon light source light-emitting elements, and single-photon measurement elements. By dividing standards for possible parts, it will be possible to help the development of the industry through standardization.

In other words, it is recommended to discuss the standard for the coupling method (e.g. socket) and the performance class of parts common to the sensor system, such as light bulb socket standard.

Achieving standards with these attributes can be challenging. Some specific challenges in the development of standards for quantum technologies include:

- **Ensuring adequate industry engagement**

Because in most countries industry engagement in the standards development process is not incentivized with government support, companies there tend to wait until there is a clear market incentive to invest significant time and resources in standards activities. This tends to favour standardization of mature technologies, and by engaging late, companies may miss the opportunity to influence standards that will in turn influence the market.

- **Creating a multi-organizational cohesive suite of standards**

There is no sovereign organization that coordinates international standards development. Any SDO, any consortium, or even any company is free to create candidate standards specifications. These candidate standards may overlap and conflict,

preventing any single standard from being broadly adopted and forcing companies to bear the financial burden of making their products compatible with multiple standards. There are already at least two efforts creating standards for quantum terminology (ISO/IEC JTC 1/WG 14 and IEEE P7130), both of which require careful review from the same limited pool of experts [72].

- **More is not better**

Initiating and promoting standards activities before the science has matured can lead to standards that lock in inferior technologies or give an unfair advantage to those quickest to take leadership. There is a temptation to equate starting or leading standards with market dominance, which can fragment the market with too many standards which may not meet real market needs. For standards to have their desired impact they must be broadly adopted and must draw expertise from a broad stakeholder community, and thus should be started and advanced with careful consideration.

Section 7

Recommendations and conclusions

7.1 General recommendations

7.1.1 – The industry and the standardization community should consider quantum information technology as a heterogeneous technology and different aspects of this technology are still evolving at different levels of maturity.

Quantum information technologies are at different levels of maturity. A robust industry will need a robust supply chain. Therefore, it is critical that industry and standardization activities do not prematurely shut down avenues of technical development or hinder technology evolution.

7.1.2 – Companies should keep aware of the continually evolving quantum standards development arena, consider potential implications for their own product development, and identify opportunities to engage.

Standards committee participation is a business decision for any industrial entity. Even if a small or medium enterprise does not feel justified to use its limited resources to participate in standards committees, it is still important that they keep aware of standards development activities to identify the impact those standards may have on their products and identify opportunities for direct involvement in standards development.

7.2 Recommendations to IEC and standard makers

7.2.1 – Ensure balanced participation and adequate industry engagement throughout the standardization process.

Robust standards are science-based but industry-driven. Many industry stakeholders will wait for a clear market incentive before investing significant time and resources in standards activities. Companies that engage later than others may miss the opportunity to influence standards that will influence the market. This can result in a disadvantaged position for these companies and can also lead to standards that do not fully address market needs.

For standards to have their desired impact they must be broadly adopted and must draw expertise and buy-in from a broad stakeholder community, characterized by a diversity of factors, including country, technical expertise (industry, academia), developers, producers/manufacturers, users, and other roles. It is important for SDOs such as IEC to engage a diverse representation of industry and obtain their input early and in a balanced manner.

7.2.2 – Proactively coordinate and collaborate with other SDOs to produce a comprehensive, robust, and consistent suite of standards to serve the global quantum marketplace.

Multiple and competing standards can confuse and fragment the market, burdening vendors and users with the need to maintain compatibility with multiple formats. Overlapping standards also tax the limited community of experts, who

are called on repeatedly to contribute and review documents. Since no single organization controls or manages the entire standards development process for quantum technologies, it is important that SDOs take the initiative to coordinate and collaborate in areas of joint interest. IEC and other SDOs should avoid replicating current international quantum-related standards development work as noted in Section 6 of this white paper but should consider those efforts as potential opportunities for collaboration.

7.2.3 – Develop a standardization strategy which distinguishes needs at the material, component, and systems level.

Robust quantum-enabled technologies, such as a quantum computer, require standardization at many levels including component characterization and measurement, interconnection among component technologies, system-level characterization and performance, and materials. The module technologies, such as atomic ion cells, diamond defect-based quantum magnetic components, single-photon-emitting elements, etc. are essential and enabling, and will need to be compatible with multiple industrial applications. Standardization activities in these module technologies will open various opportunities in the industrial applications of quantum technologies.

It is not likely that a single committee could appropriately address the significant technological diversity among all the components anticipated for quantum computing, communication, and sensing applications, and there are many existing sensor standards that will likely continue to be relevant regardless of the quantum nature of the sensor. New standards efforts should be considered on a case-by-case basis, considering standardization readiness and specific technological needs, and the IEC SMB should initiate a discussion on the standardization strategy going forward and the division of roles and responsibilities among ISO/IEC JTC 1 and the other existing technical committees.

7.2.4 – ISO/IEC JTC 1/WG 14: Quantum computing, should expand its terminology standardization effort to encompass quantum information technologies broadly.

ISO/IEC JTC 1/WG 14: Quantum computing, is currently standardizing terminology for quantum computing. Since there is significant overlap in the terminology needed across various quantum disciplines, it is recommended that the WG 14 effort be expanded to include terms needed more broadly for quantum technologies, including quantum sensing and communications.

7.2.5 – ISO/IEC JTC 1/WG 14 should be more proactive in tracking related quantum computing standardization efforts and maintaining active relationships with other relevant standards organizations.

ISO/IEC JTC 1/WG 14: Quantum computing, is tasked with developing and maintaining a list of quantum computing standards projects underway in ISO TCs, IEC TCs, and ISO/IEC JTC 1. The working group should be encouraged to continue to proactively address this task, which will help IEC and others identify other gaps and opportunities in quantum computing standardization. WG 14 also maintains active liaison relationships with many organizations, both internal and external to ISO and IEC, involved in quantum computing standardization. WG 14 is well positioned to be considered a focal point for ISO-IEC collaboration with other organizations for quantum computing.

7.2.6 – The IEC should develop a mechanism to assess the standardization readiness of emerging technologies, collaborating with organizations that share this goal.

The purpose of standardization is to promote commercialization via a fair and open global marketplace. Standards should be based on sound science but driven by industry needs and be flexible enough not to prematurely eliminate

competing technologies. A necessary condition for standardization is that industries and markets exist.

The IEC is encouraged to develop a standardization readiness assessment tool for emerging technologies that takes into account the existence and maturity of the market. To avoid multiple and competing definitions for standardization readiness, the IEC should develop this tool in collaboration with current efforts in other organizations which share this goal and with input solicited from the broader expert community via multiple channels (e.g. websites, social media, webinars, etc.).

7.2.7 – The IEC should use the standardization readiness tool as described above to assess the standardization readiness of quantum technologies for computing, communication, and sensing.

QIT is a collection of different technologies in the areas of computing, communication, and sensing. It is important for the standardization community to understand and agree upon the different standardization readiness levels (SRLs) for the different QITs to avoid premature standardization, or prematurely limiting technology development. Therefore, such activity will require an intensive collaboration with other standardization and research organizations.

The IEC should use the standardization readiness methodology they develop (see above recommendation) to assess and assign a proposed SRL to each of the identified QITs in the areas of quantum computing, quantum communication, and quantum sensing, and to recommend for which of these and where QIT standardization should take place.

The IEC SMB is recommended to create a group that conducts the evaluation of the standardization readiness and its application to QIT.

7.3 Conclusions

Future technologies will directly make use of quantum laws as the working principle in computing, communication, and sensing to go beyond the limitations of existing systems. Although current quantum technologies are imperfect, their market has already appeared because of their potential and extensive impact. Cloud-based quantum computing services are already available. Telecom companies are attempting to introduce the infrastructure of commercial quantum communication. Related sensing technologies as well as their direct applications to quantum metrology have made extraordinary progress.

This white paper introduces the current state-of-the-art QIT. Section 1 summarizes the background and the motivations of QIT from views taken at various angles. Section 2 focuses on the market for QIT and industry perspectives. Section 3 details the fundamentals of QIT. It identifies the technological status of quantum computing, quantum communication, and quantum sensing, addresses ongoing research results and markets together in perspective. Section 4 identifies near- and long-term challenges to achieving practical quantum technologies. In particular, key milestones are reviewed. Section 5 collects a list of use cases for QIT. Section 6 reviews the ongoing standardization activities. Section 7 examines some important recommendations regarding the diversity of QITs, industry participation, the role of the IEC, and collaboration with other SDOs.

QIT introduces a new ICT paradigm. It is evolving today. A technological roadmap is needed to reach the level of real-world applications. Therefore, it is important to develop QIT in such a way that fundamental science and practical applications interact with each other. The science-based and industry-focused markets for QIT will mature in the near future, sequentially by application.

Bibliography

[1] Inside Quantum Technology, Report IQT-QCS-0719: 2019, *Quantum Computing Strategies, 2019*. Available for purchase: https://www.insidequantumtechnology.com/ product/quantum-computing-strategies-2019. [Accessed: 14 October 2021].

[2] BBVA Open Mind, "Quantum Internet Explained" [Online]. Available: https://www.bbvaopenmind.com/en/technology/digital-world/quantum-internet-explained. [Accessed: 14 October 2021].

[3] SHOR, Peter, W., Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*. IEEE, 1994, pp. 124-134.

[4] HARROW, Aram, W, et al. Quantum algorithm for linear systems of equations. *Physical review letters*, 2009, 103.15: 150502.

[5] WIEBE, Nathan, et al. Quantum algorithm for data fitting. *Physical review letters*, 2012, 109.5: 050505.

[6] CHILDS, Andrew, M, et al. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision. *SIAM Journal on Computing*, 2017, 46.6: 1920-1950.

[7] Universal Quantum Simulators. *Science*, 23 Aug 1996, Vol 273, Issue 5278, pp. 1073-1078.

[8] SIBSON, P., ERVEN, C., GODFREY, M. et al. Chip-based quantum key distribution. *Nat. Commun*. 8, 13984, 2017 [Online]. Available: https://doi.org/10.1038/ncomms13984. [Accessed: 14 October 2021].

[9] "BB84", *Wikipedia* [Online]. Available: https://en.wikipedia.org/wiki/BB84. [Accessed: 14 October 2021].

[10] Toshiba, "Quantum Key Distribution" [Online]. Available: https://www.toshiba.co.jp/qkd/en/why.htm. [Accessed: 14 October 2021].

[11] Inside Quantum Technology, Report IQT-IQN-0920: 2020, *Quantum Networking: A Ten-year Forecast and Opportunity Analysis*. Available for purchase: https://www.insidequantumtechnology.com/product/quantum-networking-a-ten-year-forecast-and-opportunity-analysis/. [Accessed: 14 October 2021].

[12] DEGEN, Christian L, et al. Quantum sensing. *Reviews of modern physics*, 2017, 89.3: 035002.

[13] ACÍN, Antonio, et al. The quantum technologies roadmap: a European community view. *New Journal of Physics*, 2018, 20.8: 080201.

[14] https://www.bipm.org/en/search?p_p_id=search_portlet&p_p_lifecycle=2&p_p_state=normal&p_p_mode=view&p_p_resource_id=%2Fdownload%2Fpublication&p_p_cacheability=cacheLevelPage&_search_portlet_dlFileId=41483053&p_p_lifecycle=1&_search_portlet_javax.portlet.action=search&_search_portlet_formDate=1632145253200&_search_portlet_query=atomic+time&_search_portlet_source=BIPM. [Accessed: 14 October 2021].

[15] Quantum Flagship, “Atomic Clocks” [Online]. Available: https://qt.eu/discover-quantum/underlying-principles/atomic-clocks. [Accessed: 14 October 2021].

[16] NASA, “What Is an Atomic Clock?” [Online]. Available: https://www.nasa.gov/feature/jpl/what-is-an-atomic-clock. [Accessed: 14 October 2021].

[17] HILL, Ryan M., et al. Multi-channel whole-head OPM-MEG: Helmet design and a comparison with a conventional system. *NeuroImage*, 2020, 219: 116995.

[18] BOTO, Elena, et al. Moving magnetoencephalography towards real-world applications with a wearable system. *Nature*, 2018, 555.7698: 657-661.

[19] HILL, Ryan M., et al. A tool for functional brain imaging with lifespan compliance. *Nature communications*, 2019, 10.1: 1-11.

[20] BATTERSBY, Stephen. Core Concept: Quantum sensors probe uncharted territories, from Earth’s crust to the human brain. *Proceedings of the National Academy of Sciences*, 2019, 116.34: 16663-16665.

[21] AHMED, Zeeshan, et al. Quantum sensing for high energy physics. *arXiv preprint arXiv:1803.11306*, 2018.

[22] Britannica, The Editors of Encyclopaedia. "Gravimeter". *Encyclopedia Britannica*, 19 Jan. 2012 [Online]. Available: https://www.britannica.com/technology/gravimeter. [Accessed: 14 October 2021].

[23] Britannica, The Editors of Encyclopaedia. "Gyroscope". *Encyclopedia Britannica*, 12 Nov. 2020 [Online]. Available: https://www.britannica.com/technology/gyroscope. [Accessed: 14 October 2021].

[24] FENG, Donghui. Review of quantum navigation. *IOP Conference Series: Earth and Environmental Science*, 2019. p. 032027.

[25] NAWRAT, Aleksander, et al. Inertial navigation systems and its practical applications. In *New approach of indoor and outdoor localization systems*, Edited by Fouzia Elbahhar 2012, p. 213.

[26] Muquans, “Absolute Quantum Gravimeter” [Online]. Available: https://www.muquans.com/product/absolute-quantum-gravimeter. [Accessed: 14 October 2021]

[27] Nature, “Quantum diamond sensors” [Online]. Available: https://doi.org/10.1038/d41586-021-00742-4. [Accessed: 14 October 2021].

[28] Inside Quantum Technology, Report IQT-QS-0119: 2019, Quantum Sensors Markets, 2018 and Beyond. Available for purchase: https://www.insidequantumtechnology.com/product/quantum-sensors-markets-2018-beyond. [Accessed: 14 October 2021].

[29] ARUTE, Frank, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 2019, 574.7779: 505-510.

[30] ZHONG, Han-Sen, et al. Quantum computational advantage using photons. *Science*, 2020, 370.6523: 1460-1463.

[31] ARUTE, Frank, et al. Hartree-Fock on a superconducting qubit quantum computer. *Science*, 2020, 369.6507: 1084-1089.

[32] Quantum Computing Report, “Qubit Count” [Online]. Available: https://quantumcomputingreport.com/scorecards/qubit-count. [Accessed: 14 October 2021].

[33] MONROE, Christopher, et al. Scaling the ion trap quantum processor. *Science*, 2013, 339.6124: 1164-1169.

[34] BRUZEWICZ, Colin D., et al. Trapped-ion quantum computing: Progress and challenges. *Applied Physics Reviews*, 2019, 6.2: 021314.

[35] SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*. IEEE, November, 1994, pp. 124-134.

[36] YOST, D. R. W., SCHWARTZ, M. E., MALLEK, J., ROSENBERG, D., STULL, C., YODER, J. L., OLIVER, W. D. (2020). Solid-state qubits integrated with superconducting through-silicon vias. *npj Quantum Information*, 6(1), 1-7.

[37] GROVER, Lov K., Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 1997, 79.2: 325.

[38] IBM, “IBM’s roadmap for scaling quantum technology” [Online]. Available: https://research.ibm.com/blog/ibm-quantum-roadmap. [Accessed: 14 October 2021].

[39] OSA Industry Development Associates (OIDA), OIDA Quantum Photonics Roadmap – Every Photon Counts, 2020 [Online]. Available: https://www.osapublishing.org/abstract.cfm?uri=OIDA-2020-3. [Accessed: 14 October 2021]

[40] WEHNER, Stephanie; ELKOUSS, David; HANSON, Ronald. Quantum internet: A vision for the road ahead. *Science*, 2018, 362.6412.

[41] AWSCHALOM, David, et al. Development of quantum interconnects (quics) for next-generation information technologies. *PRX Quantum*, 2021, 2.1: 017002.

[42] AZUMA, Koji, et al. All-photonic quantum repeaters. *Nature communications*, 2015, 6.1: 1-7.

[43] PU, Yun-Fei, et al. Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments. *Nature Photonics*, 2021, 15.5: 374-378.

[44] PRESKILL, John. Quantum computing in the NISQ era and beyond. *Quantum*, 2018, 2: 79.

[45] CAO, Yudong, et al. Quantum chemistry in the age of quantum computing. *Chemical reviews*, 2019, 119.19: 10856-10915.

[46] STOUDENMIRE, E. Miles, et al. Supervised learning with quantum-inspired tensor networks. *arXiv preprint arXiv:1605.05775*, 2016.

[47] CONG, Iris, et al. Quantum convolutional neural networks. *Nature Physics*, 2019, 15.12: 1273-1278.

[48] ORUS, Roman, et al. Enrique. Quantum computing for finance: Overview and prospects. *Reviews in Physics*, 2019, 4: 100028.

[49] FARHI, Edward; GOLDSTONE, Jeffrey; GUTMANN, Sam. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*, 2014.

[50] APOLLONI, Bruno, e al. Quantum stochastic optimization. *Stochastic Processes and their Applications*, 1989, 33.2: 233-244.

[51] CASTELVECCHI, Davide. IBM's quantum cloud computer goes commercial. *Nature News*, 2017, 543.7644: 159.

[52] ABRAMSON, Norman. The ALOHA system: Another alternative for computer communications. In *Proceedings of the November 17-19, 1970, fall joint computer conference*. 1970. pp. 281-285.

[53] HUANG, Qi, et al. New type of fiber optic sensor network for smart grid interface of transmission system. In *IEEE PES General Meeting*. IEEE, 2010. pp. 1-5.

[54] DING, Yu-Yang, et al. Polarization variations in installed fibers and their influence on quantum key distribution systems. *Optics express*, 2017, 25.22: 27923-27936.

[55] WADDY, David S., et al. Fast state of polarization changes in aerial fiber under different climatic conditions. *IEEE Photonics Technology Letters*, 2001, 13.9: 1035-1037.

[56] TAROKH, Vahid, et al. Space-time codes for high data rate wireless communication: Performance criterion and code construction. *IEEE transactions on information theory*, 1998, 44.2: 744-765.

[57] EMS Element Management System [Online]. Available: http://www.ktword.co.kr/test/view/view.php?m_temp1=1695 (in Korean). Accessed 14 October 2021].

[58] HERRERO-COLLANTES, Miguel, et al. Quantum random number generators. *Reviews of Modern Physics*, 2017, 89.1: 015004.

[59] GISIN, Nicolas, et al. Quantum cryptography. *Reviews of modern physics*, 2002, 74.1: 145.

[60] Computer Security Resource Center, “Post-Quantum Cryptography” [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed 14 October 2021].

[61] ETSI, Quantum-Safe Cryptography (QSC) [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Accessed 14 October 2021].

[62] CRYPTREC, Cryptology Research and Evaluation Committees [Online]. Available: https://www.cryptrec.go.jp/en/index.html. [Accessed 14 October 2021].

[63] CRYPTREC, Investigation Reports on Cryptographic Techniques [Online]. Available: https://www.cryptrec.go.jp/en/tech_reports.html. [Accessed 14 October 2021].

[64] DIN, ISO/IEC JTC 1/SC 27/WG2 SD8 Post-Quantum Cryptography [Online]. Available: https://www.din.de/ en/meta/jtc1sc27/downloads (then choose SC27WG2 SD8). [Accessed 14 October 2021].

[65] DEGEN, Christian L.; REINHARD, F.; CAPPELLARO, Paola. Quantum sensing. *Reviews of modern physics*, 2017, 89.3: 035002.

[66] BORDÉ, Ch J. Atomic clocks and inertial sensors. *Metrologia*, 2002, 39.5: 435.

[67] KOLATSCHEK, S. et al. Bright Purcell Enhanced Single-Photon Source in the Telecom O-Band Based on a Quantum Dot in a Circular Bragg Grating. *Nano Lett*. 2021, 21, 18, 7740–7745, September 3, 2021 [Online]. Available: https://pubs.acs.org/doi/10.1021/acs.nanolett.1c02647. [Accessed 14 October 2021].

[68] HADFIELD, Robert H., et al. Single photon source characterization with a superconducting single photon detector. *Optics Express*, 2005, 13.26: 10846-10853.

[69] High speed prototype quantum key distribution system and long term field trial. *Optics Express* Vol. 23, Issue 6, pp. 7583-7592, 2015 [Online]. Available: https://www.osapublishing.org/oe/abstract.cfm?uri=oe-23-6-7583. [Accessed 14 October 2021].

[70] RUF, M., WAN, N., CHOI, H., ENGLUND, D. and HANSON, R. Quantum networks based on color centers in diamond. *Journal of Applied Physics* 130, 070901 (2021) [Online]. Available: https://doi.org/10.1063/5.0056534. [Accessed 14 October 2021].

[71] BSI, "What is a standard?" [Online]. Available: https://www.bsigroup.com/en-ID/Standards/Information-about-standards/What-is-a-standard. [Accessed: 14 October 2021].

[72] IEEE, [Online]. Available: https://standards.ieee.org/develop/project/7130.html. [Accessed 14 October 2021].

ISBN 978-2-8322-1040-4

CHF 50.-

International Electrotechnical Commission

3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
info@iec.ch
www.iec.ch

IEC WP QIT:2021-10(en)