2 Quantum Info-Communication Technology -Overview-

Masahiro TAKEOKA, Kouichi SEMBA, and Masahide SASAKI

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

1 Introduction

There have been, and will continue to be startling evolutions in information communication technologies almost on a daily basis, On the other hand, it has been pointed out that they may hit performance limitations sooner or later if conceived on the basis of conventional technological systems and their extensions. Ensuring security is the challenge of utmost importance in the rapidly expanding current-day communication networks — from land-based optical fiber networks to satellite communications — and encryption is the key for security. However, it has been pointed out that the encryption schemes currently in use may fall victim to the decoding power of future computer technologies. In other aspects, physical upper limits of the laser power injectable into optical fiber will make it harder to cope with the ever-increasing volume of communication traffic, and, on the flipside, lower limits of feeble signal identification set the threshold to the possible range of ultralong distance communication — typically communication with planetary exploration spacecraft.

Against these odds, a series of predictions have been made in recent years that may provide breakthrough technological innovations. Namely, quantum information technology can pave the way for the realization of such realms as: quantum cryptography that provides levels of security unattainable through conventional technologies, quantum computers that crunch problems that would take thousands of years if conventional computers were employed, and quantum receiving techniques that can make the ultimate physical limits of communication volume a reality. Quantum information technology (QIT) takes advantage of cutting-edge quantum physics theories that explain the microscopic behaviors of atoms, electrons and photons. Since the advent of the 21st century, serious research and development has been underway toward realization of the technology worldwide. NICT has been promoting research toward realization of quantum information technologies placing special focus on their communication aspects — i.e. Quantum Information and Communication Technology (QICT). This report overviews the current status of research and development in NICT.

2 Quantum photonic network technology

Cryptography is used in various scenes in our modern society. However, it has been constantly warned that the current cryptographic methods may be vulnerable to decryption if some innovation takes place in the future in the art of computing. The concern stems from the fact that the security of software-based modern cryptography depends heavily on the intensive computation required to decrypt the encrypted message (so-called “computational security”). For example, the RSA cryptosystem — one of the representative techniques in modern cryptography — is built on the rationale that modern computers consume too much time to factorize a large number into prime factors. However, rapidly growing computing power and an invention of an innovative prime factorization algorithm may enable a computer system to solve the problem in a reasonably manageable timespan in the near future. It is already in our knowledge that realization of quantum computing, computing technology that takes advantage of quantum characteristics, can crunch the RSA code easily and quickly. The situation poses serious threats to such areas as national intelligence, financial and medical information

where long-term absolute security in confidential communications is essential. Quantum cryptography is the branch of information and communication technology (ICT) that promises to deliver the hoped-for tools.

The two major features of quantum cryptography in comparison with the existing methodologies can be described as follows: information-theoretic security that defies any eavesdropping attempts from any third party in possession of whatsoever huge computing power, and the detectability of any physical eavesdropping attempt (e.g. partial tapping of information from the optical fiber). Quantum cryptography consists of two major elements: Quantum Key Distribution (QKD) that allows sharing of the secret key (sequence of random bits shared only among the senders and receivers), and the encrypted communication using QKD. In the latter process, the information to be sent is encrypted using the QKD-shared secret key before being transmitted through one of the standard paths (i.e. the internet).

QKD requires special communication devices that become available only with the help of quantum characteristics. The sender transfers information in the form of specially randomized photons, i.e. particles of light. The receiver detects the state of the photons one by one, and rejects those with suspicion of eavesdropping with the help of an algorithm on the computer. This process (key distillation) enables the receiver to generate a secure secret key. Any eavesdropping attempt to a photon level signal infallibly leaves a vestige of tapping (Heisenberg's uncertainty principle), which can be used to detect the attack. In addition, the use of physical random number generation (a stochastic physical phenomenon is used to generate random numbers) enables sharing of information-theoretically secure secret keys (i.e. security totally unaffected by the level of computing capability on the side of the eavesdropper). This has been an overview of the principle that supports quantum cryptography. In the era when quantum cryptography was invented (from the 1980s to 1990s), it was generally accepted that exactly one photon must be prepared to investigate the signal conveyed by the single-photon state. However, subsequent theoretical studies have shown that a very weak laser light (such that the laser pulse contains only one or less photons on average) and well-contrived transmitting/receiving devices can deliver a substitute for single-photon experiments. Entering this century, these findings have significantly accelerated research and development toward practical realization of quantum cryptography.

NICT started basic research on quantum cryptography in 2001 in collaboration with industries and universities. Since 2006, NICT has been conducting application studies including demonstration of a quantum cryptography network based on a ground fiber network, and toward practical application thereof. In addition to the effort to realize quantum cryptography systems, the research in recent years has indicated the possibility of delivering new security technologies even to communication networks which defy, at least at present, implementation of quantum

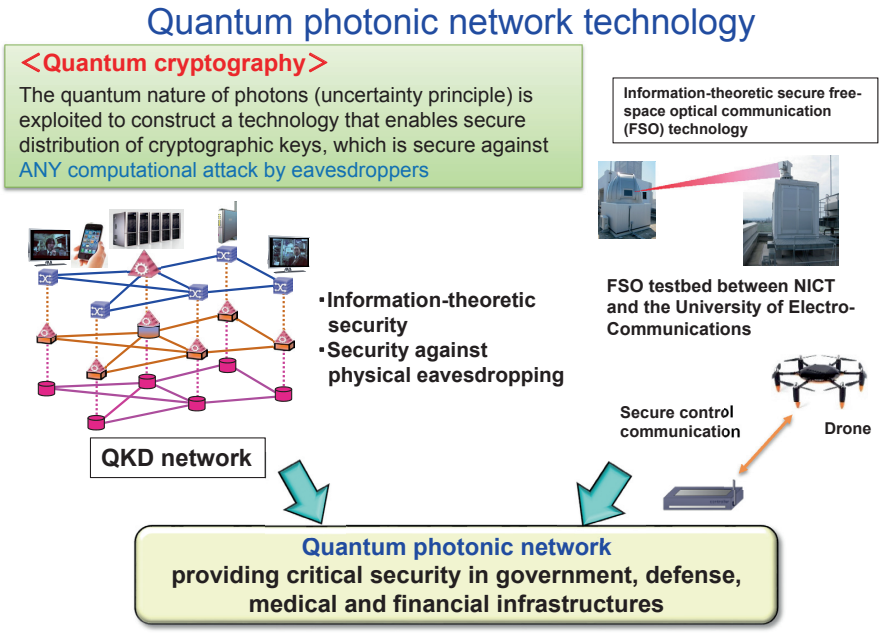

Fig. 1 Overview of quantum photonic network technology

cryptography. These include communication with drones and the Internet of Things (IoT), where one or more of the element technologies for constructing a quantum cryptography system — very week photonic communication, key distillation, physical random number generation, and others — have effect. We call these technologies collectively "quantum photonic network technology" (Fig.1).

3 Quantum node technology

We are now enjoying a seemingly sufficient amount of information transfer provided by optical communication. However, as mentioned in the introduction paper, concerns are rising over the possibility that the rapidly growing communication volume may hit the theoretical ceiling sooner or later. Our current technology is faced with another challenge: in ultralong distance communication paths in outer space, where optical amplifiers are not available, technology to extract the maximum amount of information from ultraweak signals buried in quantum noise is not yet within reach. Turning our eye to security issues, quantum cryptography described in the previous section can be the agent to realize ultimate security. However, because it involves transmission and reception of photonic level signals, the QKD protocols now under development toward practical implementation impose heavy restrictions in terms of communication distance and key generation rate.

A drastic solution to address these problems can be derived from a technology that measures, controls and preserves the quantum attributes of the photonic signal at each relay point (node) of the network. In reality, extreme fragility of quantum mechanical attributes means the technology is still in need of several innovations. We call these technologies in need collectively "quantum node technology," and we are now engaged in basic research with a view toward the long-term perspective (Fig.2). Specifically, NICT is conducting research focusing on three major themes:

Quantum optical control technology: full control of the quantum state of light and establishment of a quantum-based information-communication protocol, which lies beyond the scope of conventional electromagnetic theory based optics (called classical optics in contrast to quantum optics).

Quantum metrology: control of atoms and ions on a particle-by-particle basis in view of applying them in quantum communication and the next generation frequency standards.

Superconducting quantum circuit technology: precise control of photon-matter interaction on a photon-by-photon basis on the superconducting circuit, which can be considered itself as a macroscopic embodiment of an artificial atom, in view of shedding light on hitherto unknown quantum physical phenomena. All these themes represent future technologies that directly involve cutting-edge developments in quantum physics, leading to the way to realize technologies still out of reach of the human race.

Quantum entanglement is one of the key concepts in the development of quantum technologies. It represents a correlation between particles that appears only in the quantum mechanical domain and is totally inexplicable in terms of classical physics (i.e. conventional mechanics and electromagnetism). For example, if two photons are prepared to have the same longitudinal polarization, correlation (in the classical meaning) is formed between the photonic polarization. This correlation can be detected, for example, when measurement is made for each photon by passing it through a filter capable of distinguishing longitudinal and horizontal polarization. However, measurement of different polarization bases, for example right-hand/left-hand circularly polarized light, cannot give definite correlation because each individual photon rotates in a random manner. In contrast, if photons are quantum mechanically entangled, the correlation always appears, which is irrespective of the choice of the measurement, longitudinal/horizontal polarization measurement or circular polarization measurement. A noteworthy feature of this measurement is the fact that we get the same result even if we choose the measurement method after the quantum state was prepared.

This retention of correlation under operation of any measurement method is the most peculiar feature of quantum entanglement. By monitoring the entangled photon pair using more than one measurement method, any eavesdropping attempt done to the pair by a third person can be detected 100% even after it has been delivered to two, mutually far apart receivers. A drawback of quantum entanglement is its fragility, which makes it unfit for direct long-distance transmission. This can be fixed, however, by implementing a regenerative function at the relay points in the network: partially corrupted quantum entanglement can be restored at the relay points for long-distance transmission. Realization of such quantum repeater technology will enable ultralong distance delivery of entangled photons with the same assurance of security using the field-proven QKD methods. Quantum entanglement is also known to

constitute an essential resource for quantum computers that perform parallel computing simultaneously.

Each research theme conducted in NICT aims at establishing technologies to control entanglement relations at will — i.e. entanglement between photons (quantum optical control), entanglement between atoms (quantum metrology), and entanglement between a photon and a superconducting artificial atom (superconducting quantum circuit). Note that establishing quantum entanglement is not the sole objective of these research projects (for detailed descriptions, see each corresponding paper in this special issue). In a superconducting quantum circuit system, entanglement-enabled photon-artificial atom coupling can be made extremely stronger than in any other physical system. The "deep strong coupling" may lead to the development of a new physical phenomenon no one has ever observed before.

4 Toward widespread deployment of QICT across society

Quantum technologies hold huge potential to renew our society in such aspects as the provision of ultimate safety and ultra-fast computing. In many cases, however, the prognosis is that their promises will become practically feasible only when they are properly combined with one or more existing instances of ICT. In the 4th mid/long-term plan of NICT, we adopt fusion between QICT and modern ICT as one of the themes, in view of applying QICT (and the technologies derived therefrom) to various ICT applications currently in place in society (Fig.3).

As mentioned in this paper, quantum cryptography can provide levels of security not reachable by the currently available techniques. This does not translate into total replacement of modern security technologies by quantum cryptography; its full capacity is considered to be exploited by incorporating it in the portions of modern security technology where it needs enhancement the most. For example, incorporation of quantum cryptography into the secret sharing process, a well-known technique used in modern security technologies, will help realize ultralong-term secure data center networks. In concrete terms, quantum cryptography is applied to mutual communications among distributed data storages to guarantee the total information-theoretical security of the network system.

To pursue this research and development, close collaboration with the expert researchers in modern security technology is essential. Incorporation of quantum cryptography and the related technologies derived therefrom into multi-faceted free-space communications — such as optical communication with satellites and control of drones — requires collaboration with experts in each field. Such joint efforts can only pave the way for meaningful social implementation that properly meets the requirements and specifications. NICT is also working toward developing quantum node technology, although still in the stage of basic research and in need of introducing cutting-edge ideas from other areas of ICT, targeted at such challenges as coherent light communication, silicon photonics, and

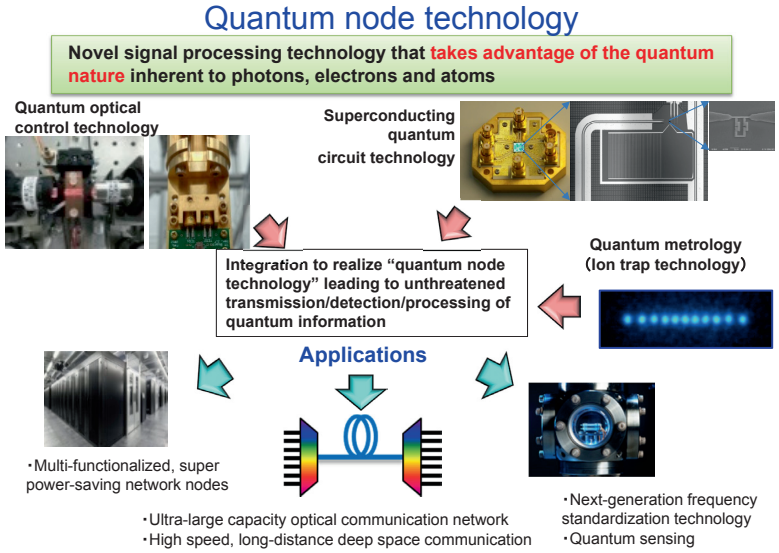

Fig. 2 Overview of quantum node technology

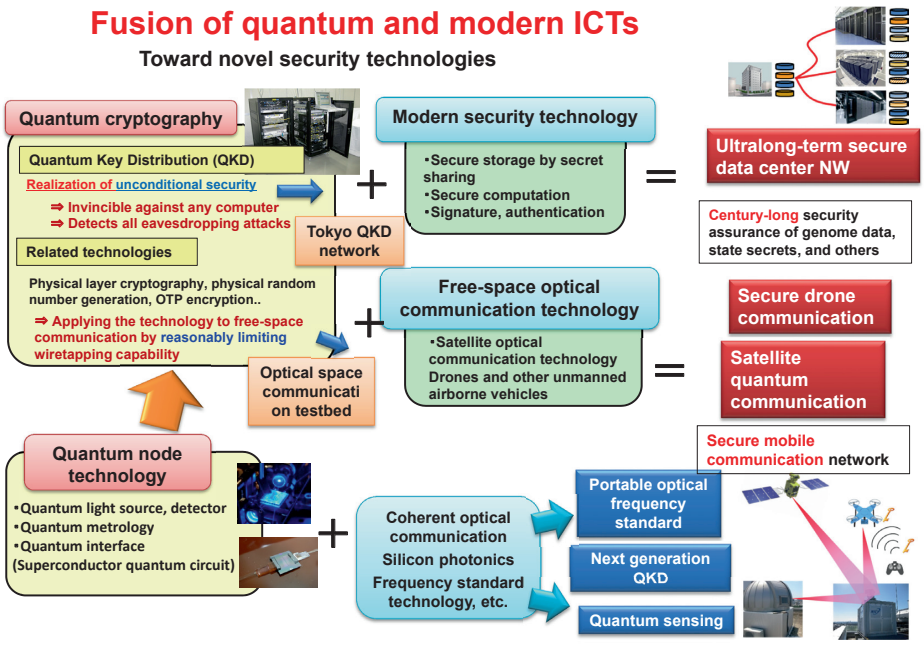

Fig. 3 Toward widespread acceptance of QICT across society

frequency standards. NICT is gearing up to develop unique technologies in these areas to support future development of ICT. In this special issue, the current status of research and development for each technical challenge is described, where the main focus is placed on those undertaken in NICT.

Masahiro TAKEOKA, Ph.D

Director, Quantum ICT Advanced Development Center, Advanced ICT Reseach Institute
Quantum optics, Quantum information theory

Kouichi SEMBA, Dr. Eng.

Executive Researcher, Frontier Research Laboratory, Advanced ICT Research Institute
Superconducting quantum electronics

Masahide SASAKI, Ph.D

Distinguished Researcher, Advanced ICT Research Institute
Quantum communication, Quantum cryptography