R&D Trends and Future Prospects of Quantum Cryptography

Masahiro Takeoka
Director
Quantum ICT Advanced Development Center, Advanced ICT Research Institute
National Institute of Information and Communications Technology

Mikio Fujiwara
Research Manager
Quantum ICT Advanced Development Center, Advanced ICT Research Institute
National Institute of Information and Communications Technology

Masahide Sasaki
Distinguished Researcher
Advanced ICT Research Institute
National Institute of Information and Communications Technology

1. Introduction

The information and communication technology that supports our modern network society has undergone remarkable development, and continues to advance every day. However, it has also been pointed out that the extension of conventional technology systems is liable to be impeded by the fundamental performance limits in the future. Quantum communication techniques exploit the properties of quantum mechanics (the physics of microscopic phenomena, such as the behavior of atoms, electrons, and photons) to their utmost potential. They are predicted to be used in variety of applications including unbreakable security techniques, ultra-long-range high-speed space communication, ultra-precise timing synchronization and sensing. As a result, the research and development of quantum communication is advancing all around the world. Although many of these are still at the stage of basic research, in this paper we introduce the current state of progress and the efforts being made in Japan and overseas with regard to quantum cryptography, which is one of the most mature applications in the field of quantum communications.

2. Quantum cryptography

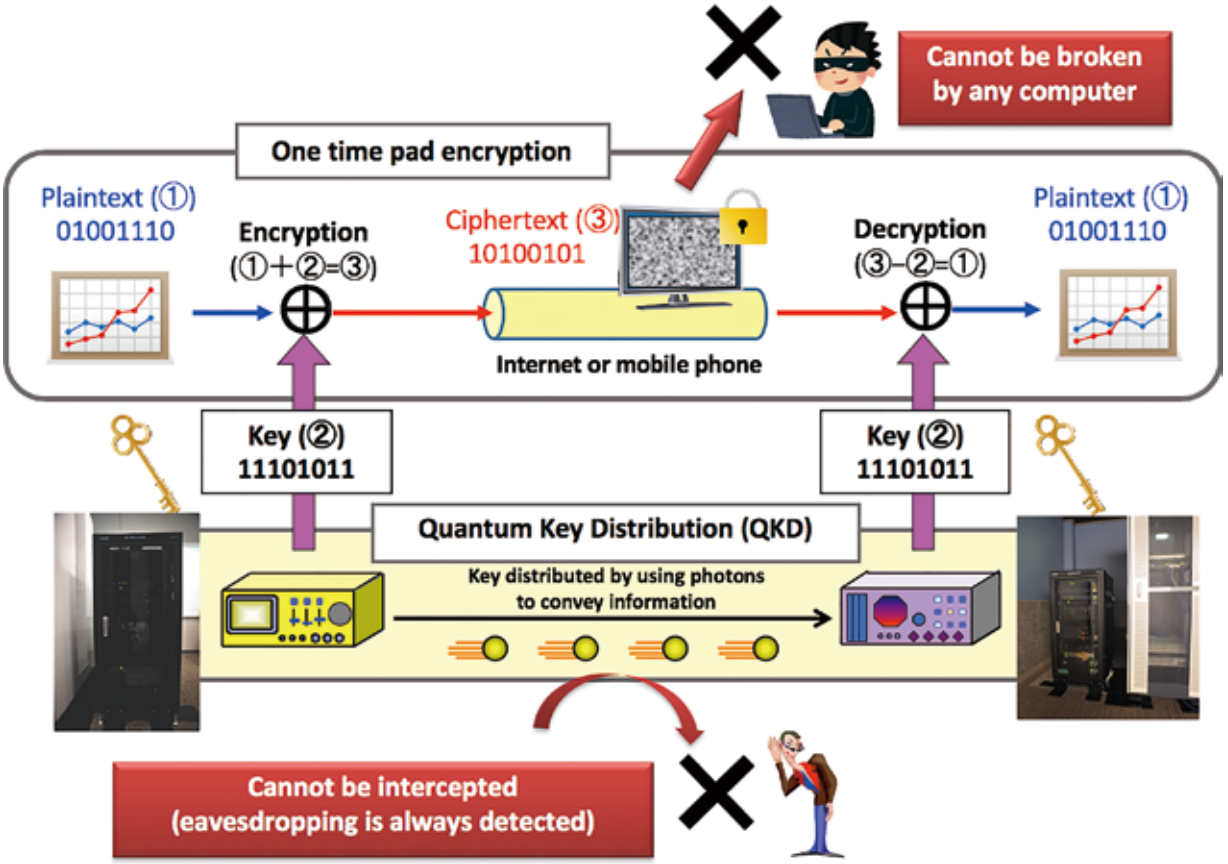
Cryptosystems based on mathematical algorithms such as RSA and elliptic curve cryptography are currently in widespread use throughout society. But although they are extremely easy to use, they are at risk of being broken by future developments in computer technology. The relationship between the performance of supercomputers and the amount of computation required to break RSA has already been estimated[1]. In addition, if recent rapid progress in R&D leads to the implementation of large-scale quantum computers, it could become possible to break these ciphers instantaneously. Furthermore, even if mathematical cryptosystems cannot be broken with existing computers, it is possible to intercept and store encrypted data so that it can be broken at a later date when sufficiently powerful computers have become available. This poses a serious potential threat to the communication of information such as state secrets and medical information (e.g. genomic data), which must provide the highest degree of security for many decades.

The security of quantum cryptography is not based on the difficulty of solving mathematical problems, but on quantum mechanics and statistics. As a result, quantum cryptography is the only current encryption method that is essentially impossible to break with computers of any kind, including quantum computers. This security is called "information-theoretic security" to distinguish it from computational security. In other words, if quantum cryptography is implemented appropriately, then it can provide absolute security that can never be broken regardless of future advances in computer technology and mathematics.

Figure 1 shows an overview of how quantum key distribution (QKD) is used to generate cryptographic keys in quantum cryptography, and how these keys are used to perform encryption*. In QKD, a random number that forms the basis of a key is delivered by transmitting a very weak optical pulse signal through

* There are several methods for encryption using keys created by QKD, but to achieve information-theoretic security, i.e. security unbreakable by any computing attacks, it is necessary to use "one-time pad encryption" where one data bit is encrypted using one key bit, and the same key bit is never used twice. Therefore, when we say that quantum encryption offers "perfect information-theoretic security," we are referring to the use of QKD + one-time pad encryption

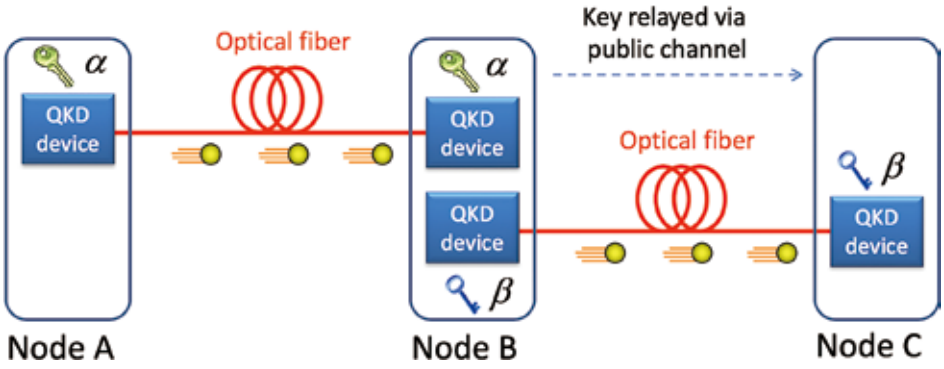
Figure 1: Overview of secure communication based on quantum cryptography (Photo: NEC's QKD transceiver)



a channel, typically an optical fiber, so that it contains on average only one photon (the smallest unit of light energy) per pulse (in standard optical communication, roughly 100,000 to 1,000,000 photons are contained in one pulse). The quantum nature of light is strongly apparent in a single-photon-level signal of this sort. One of the properties of QKD is that any attempt to eavesdrop by measuring signals en route will leave a detectable trace due to the uncertainty principle (one of the basic principles of quantum mechanics). As a result, it is possible to judge whether or not the signals have been tampered with, and to use only signals that are guaranteed not to have been intercepted. This allows keys to be shared with perfect security. Also, since the random number obtained as a key can be set to any desired sequence, one can use random numbers with no mathematical structure such as physical random numbers to make the key unbreakable by any computational attack. In this way, it is possible to detect any kind of physical eavesdropping during key distribution, allowing data to be encrypted with perfect security that cannot be broken by any computer. An actual QKD device consists of a photon transceiver combined with electrical components, e.g. a signal processing board that performs error correction and privacy amplification on the key information. The key itself is a binary sequence of zeros and ones, and after the key has been shared, it is used for data encryption/decryption and transmission via ordinary computers and communication channels, such as the Internet.

QKD overcomes the fundamental problem of mathematical cryptography, and can in some sense provide ultimate security. But on the other hand, there are also major restrictions on the implementation of QKD. Photons are easily lost due to transmission losses in communication channels, and it is not possible to use optical amplifiers (which are essential for long-distance fiber communication) because they destroy the quantum state of the signal. For this reason, the transmission range of a single QKD transceiver in fiber communication is limited to around 50 to 100 km. Furthermore, the key generation rate per wavelength is currently limited to the range of kilobits per second to megabits per second (depending on distance and device performances). It is expected that improvements will be made to some extent such as wavelength division multiplexing and other technical advances. A more fundamental challenge is to develop a novel technology called a "quantum repeater", which in principle can work as a repeater (amplifier) for quantum signals.

Figure 2: A QKD network where keys are relayed via trusted nodes



A quantum repeater must perform optical quantum computing on the transmitted signals, which is something that cannot be realized without further technological breakthroughs. Therefore, current QKD networks relay keys by connecting QKD paths between trusted nodes (i.e., nodes that are guaranteed to be secure; see Figure. 2). Although it is possible to construct a QKD network of any configuration in this way, the security of each relay station (trusted node) must be strictly guaranteed.

3. R&D trends in Japan and abroad

Thus, although quantum cryptography is still at a developmental stage, it is being actively researched and developed all over the world due to its ability to offer a level of security that is not attainable with conventional cryptography. This section introduces the R&D trends relating to the implementation of QKD in the field (for technical details and references, see, e.g. [2, 3]).

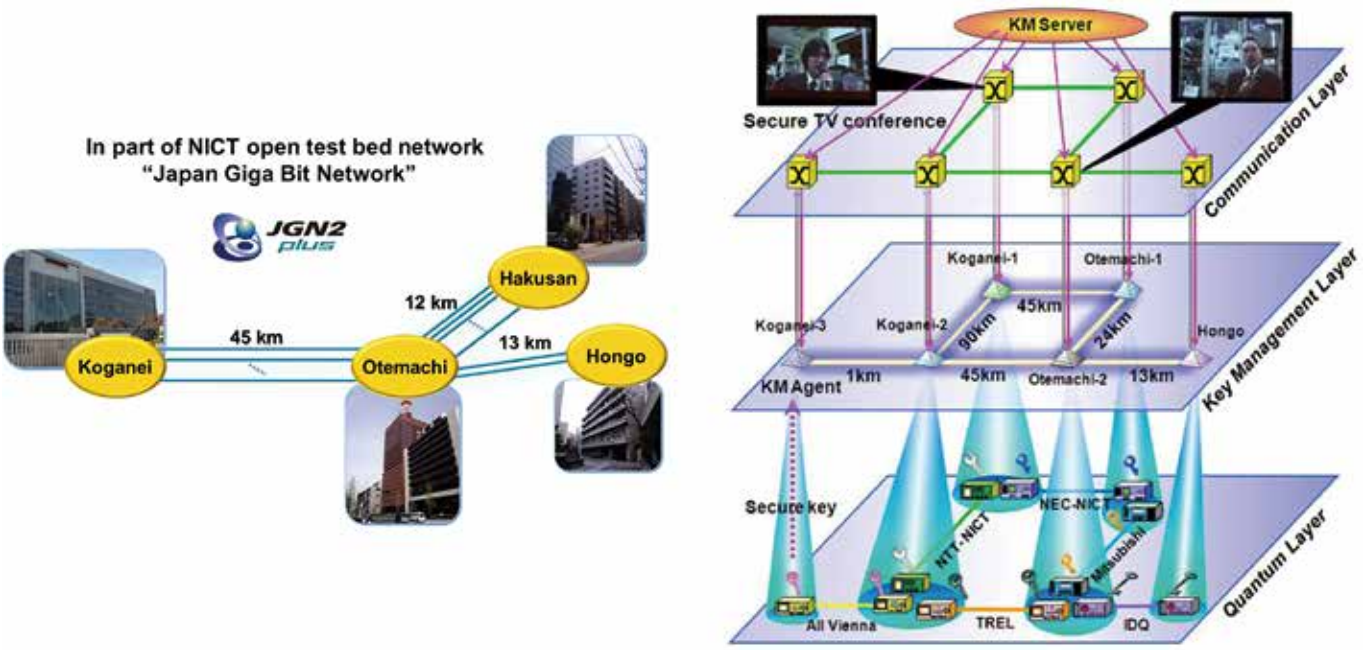
In 2004, using a terrestrial fiber-based QKD network, the Quantum Network project of the US Defense Advanced Research Projects Agency (DARPA) demonstrated the world's first metropolitan QKD network connecting three locations about 10 km apart in the Boston area. In 2008, the European Union's SECOQC (Secure Communication based on Quantum Cryptography) project set up a QKD network to connect six points in Vienna City, and they demonstrated that this allowed keys to be generated at about 1 kbps over a range of 30 km to support encrypted voice communication (phone lines) and other forms of encrypted communication. They also succeeded in interconnecting QKD devices based on different methods developed by multiple research organizations.

In Japan, the Ministry of Internal Affairs and Communications and the National Institute of Information and Communications Technology (NICT) have been promoting public–private collaboration projects, and in 2010, they built the Tokyo QKD Network from 100 kbps class QKD devices capable of generating keys a hundred times faster than earlier systems. As a result, they were able to perform the world's first demonstration of secure video transmission (video conferencing) based on QKD. Unlike the two earlier networks, the Tokyo QKD network remains operational to this day, and has been used to promote the development, trial operation and network testing of QKD devices developed by various Japanese research organizations. It is currently being used to transmit data for a distance of 50 km at approximately 1 Mbps, which is the world's highest performance for equipment deployed in the field. The project also developed QKD platform technologies, including key management platform technology for the secure and proper management of QKD networks and interfaces for supplying keys to the application layer in a suitable manner. These are necessary in practical applications of the QKD networks. QKD technology developed and tested in the Tokyo QKD Network has been deployed to actual user environments. Since 2015, NEC uses it to protect an in-house link between cybersecurity-related facilities, and Toshiba used it to protect the 7km data transmission link between the Toshiba Life Science Analysis Center and Tohoku University's Tohoku Medical Megabank Organization in Sendai.

Meanwhile, the progress made by China in recent years has been remarkable. Over a period of about three and a half years, China has constructed the world's largest QKD network connecting Beijing and Shanghai with 32 trusted nodes spread over a distance of about 2,000 km. This network has been operating since 2017. National projects to construct QKD networks are also under way in other countries including the UK and Italy, and quantum cryptography businesses in the US has announced plans to construct a QKD network service between Boston and Washington DC. In this way, the R&D and implementation of such networks remains competitive.

QKD can operate not only on optical fibers but also in free-space optical communication. For example, it is difficult to realize inter-continental ultra-long-distance key distribution (e.g., between Japan and the US) via a terrestrial QKD network connected via trusted nodes. However, the space environment of artificial satellites has a very thin atmosphere and can be used for communication with very low losses. Studies aimed at implementing satellite QKD are being pursued in several countries. In 2017, China succeeded in the first ever key generation by QKD between a satellite and a ground station. It also succeeded in key distribution via satellite between China and Austria, and demonstrated the encrypted transmission of a 5 kB image using this key. Meanwhile, in Japan, NICT is looking at

Figure 3: The Tokyo QKD Network (left) and QKD platform (right) constructed in 2010 [4]. See [5] for the current network operating status.



ways of implementing practical technology for the future, and has conducted a basic experiment (transmission and reception of weak photon-level signals) to demonstrate the world's first quantum communication using a microsatellite that has less than one tenth the mass of the Chinese satellite and is more cost-effective. Satellite quantum cryptography projects have been started in countries all over the world, and it is expected that competition in this field will become more intense in the future.

4. Integrating quantum cryptography with modern security technology: Data storage network based on QKD and secret sharing

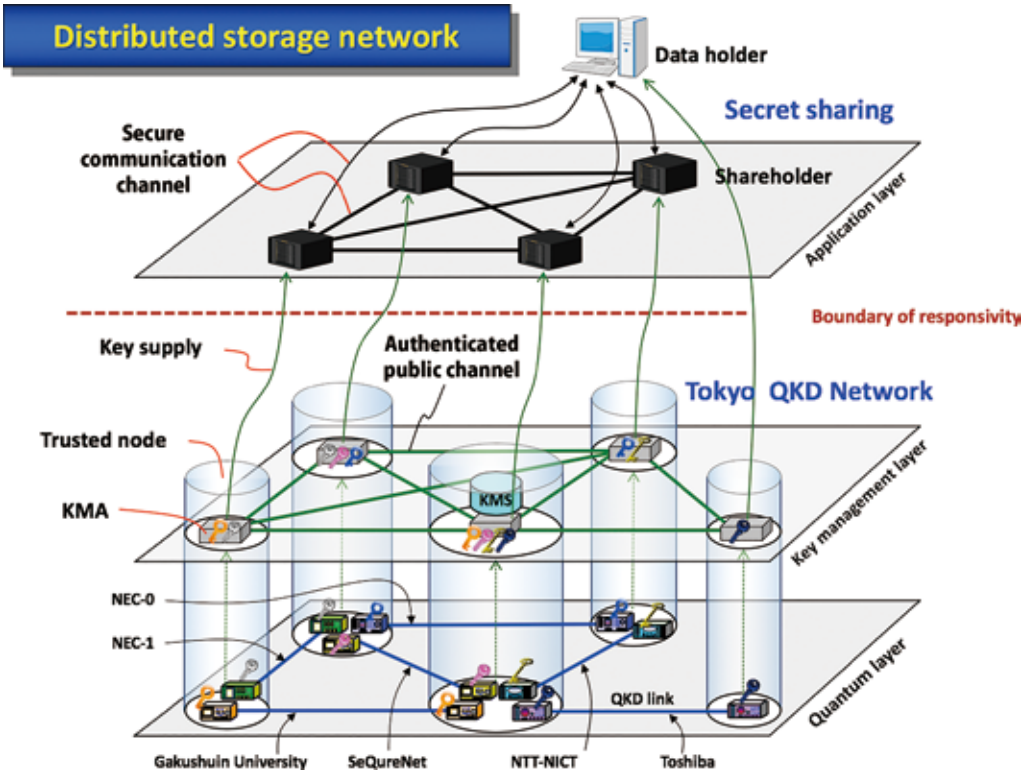
Although QKD guarantees unbreakable security during data transmission, it does not protect data in storage. However, in modern cryptography, there is a method called secret sharing whereby data is divided and encrypted before it is stored. For example, in Shamir's (n, k) threshold distribution method, the original data is divided into n shares that are separately encrypted. The original data can be restored by collecting k or more of these n shares, but with fewer than k shares, it is not possible to recover the original data using any computer; in other words, it has the information-theoretic security. Therefore, if data is distributed and stored in n separate locations, then it will still be information-theoretic secure even if part of it is stolen. Conversely, even if a part of the data is lost due to a natural disaster or the like, the information can still be recovered. This is an excellent mathematical algorithm that can be used to simultaneously save and backup secret data. However, it does not answer the question of how data shares can be securely transmitted to the distributed storage. In other words, if QKD and secret sharing can complement each other in the transmission and storage of data, then it will be possible to realize the security potential of secret sharing, resulting in a network that offers information-theoretically secure storage throughout the entire system.

Using five nodes on the Tokyo QKD Network, NICT and the Tokyo Institute of Technology have built a QKD secret sharing storage network that implements the secret sharing protocol described above. We also developed a protocol whereby information-theoretically secure authentication can be performed with a single password, and we were the first in the world to conduct a successful demonstration test of information-theoretically secure authentication, transmission, storage and recovery ([6] and section 3-2 of [2]). It is expected that this sort of distributed storage will be made publicly available in the near future as a way of creating backups to deal with disasters such as earthquakes and fires while at the same time providing the high level of security needed for confidential information such as medical records. If it is possible to construct a QKD network for distributed storage over an area of 50 to 100km, it would provide an effective system for storing secret backups that can withstand large earthquakes and tsunamis.

5. Standardization

Following the European SECOQC project, the European Telecommunications Standards Institute (ETSI) set up an Industrial Specification Group (ISG-QKD) to hold comprehensive discussions of QKD devices and to discuss details including the application interfaces and implementation security (security taking actual device performance and physical properties into consideration). Although the ETSI

Figure 4: A secret sharing storage network using QKD [2, 6].



has been actively working on QKD standardization for a long time, discussions of standardization have only started very recently at other standards organizations. This year, in the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T), study groups SG13 and SG17 issued proposals for technologies including a QKD network framework and network security. The International Organization for Standardization (ISO/IEC) has also produced a technical report on the subject. In China, a comprehensive framework for quantum communication technology is being discussed by the China Communication Standardization Association (CCSA). It is expected that active discussions and liaisons will continue in the future.

6. Conclusion

Although quantum cryptography cannot be deciphered by any computer and it can provide perfect security when properly implemented, it also involves practical difficulties such as high implementation costs and limitations in terms of distance and speed that do not apply to mathematical cryptosystems. For this reason, the social implementations of quantum cryptography are expected to start with high-end technology applications. Progress is also being made in the development of applications that uses technical components QKD, such as physical random number sources and key management/operation architectures. Meanwhile, mathematical cryptosystems are incorporating new technologies such as post-quantum cryptography which only provides computational security but is believed to be secure against attacks by quantum computers. Going forward, it will be essential to apply these various security technologies including quantum cryptography in an appropriate way by conducting R&D aimed at total solutions that provide the required security where it is needed in overall systems.

References

[1] CRYPTREC "Cryptographic Technology Evaluation Committee", 2013.

[2] "Special issue: Quantum data communication", Journal of National Institute of Information and Communications Technology, Vol. 64, No. 1 (2017).

[3] M. Fujiwara, A. Carrasco-Casad, T. Kitamura, M. Sasaki, M. Toshima: "Experimental optical communication between an ultra-small satellite and earth aiming for quantum communication", 38th Quantum Information Technology Study Group QIT2018–17, 2018.

[4] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD Network", Opt. Express, 19, 10387 (2011).

[5] The Project UQCC (Updating Quantum Cryptography and Communications). http://www.uqcc.org/

[6] M. Fujiwara et al., "Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing", Sci. Reports, 6, 28988 (2017).

Cover Art

Seki Sanjuro (Picture of kabuki actor Seki Sanjuro.)

Utagawa Toyokuni (1769-1825)

Collection of the Art Research Center (ARC)
Ritsumeikan University
Object number: arcUP3547