Quantum Cryptography and Quantum Key Distribution Network

Toward social deployment of computationally unbreakable cryptosystems

TAKEOKA Masahiro

Research Executive Director, Advanced ICT Research Institute

He joined CRL (currently NICT), Japan, in 2001. His research interests include quantum optics, quantum information theory, and quantum cryptography. Since April 2021, he has been a professor of at Keio University, and also a research executive director at Advanced ICT Research Institute of NICT.

The conventional cryptography that underpins today's information society is facing the risk of decryption as quantum computers become more powerful. Meanwhile, quantum cryptography is currently the only cryptographic system that has been mathematically proved to be impossible to decrypt with any computer, including future large-scale quantum computers. We take a look at the efforts and future prospects for research and development, and the implementation of a quantum key distribution network, which is the core technology of quantum cryptography.

Cryptographic technology which underpins today's networked society, and its issues

The security of the cryptography that is widely used today is guaranteed by "computational security," which means that extremely massive computing power is needed for decryption. This allows us to safely exchange data every day. However, today's cryptography is facing the potential threat of becoming easily decrypted due to the advent of large-scale quantum computers and entirely new computational technology/mathematical algorithms in future. Especially, critical information that requires secrecy for decades is at risk of "harvest now, decrypt later" attacks, in which encrypted data is eavesdropped or acquired, and then decrypted in future when new computational technology is developed. This is why an urgent response is required.

Two new types of technology are being developed to address this issue. One is "post-quantum public-key cryptography," which has the same computational security but has a mathematical structure that is thought to be difficult to decrypt with currently known quantum calculation algorithms, and it is now being implemented and standardized. The other type is quantum cryptography, as explained below. Quantum cryptography is currently the only cryptographic system that has been proved to be safe and impossible in theory to decrypt with any computational technology or computers in future ("information-theoretic security").

Quantum cryptography and quantum key distribution (QKD) network

As shown in Figure 1, quantum cryptography consists of two steps: quantum key distribution (QKD) and one time pad (OTP) encryption. QKD is a technology for the sender and receiver to share a secret key that is kept secure against third parties, which uses quantum mechanical properties of light signals, such as photons. OTP encryption encrypts data using an encryption key having the same size as the data and, once a key is used, it will not be reused. Using the encryption key provided by QKD achieves information-theoretic security. OTP encryption and the sending and receiving of encrypted data are all performed with normal computers and communication lines; only the QKD part requires quantum technology.

The technology for managing and distributing keys safely and efficiently by connecting QKD transceivers to the network is called a quantum key distribution (QKD) network (Figure 2). By sharing the encryption key at any point on the network with the QKD network, and providing the key to the conventional network, it is possible to provide new security services using an information-theoretic secure cryptographic key. In addition to QKD networks connected with optical fibers, QKD using satellite communication is also under development, which is expected to be integrated into a global QKD network in future.

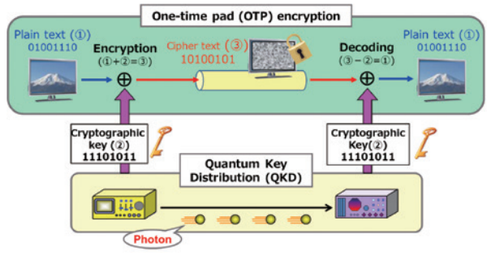

Figure 1 Mechanism of Quantum Cryptography

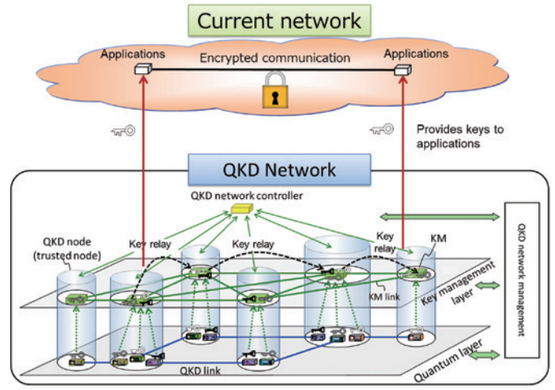

Figure 2 Key delivery from Quantum Key Distribution (QKD) Network

Research and development, and efforts toward implementation

Since the 2000s, in collaboration with universities and companies, NICT has been developing the technology for QKD systems and their networking technologies, such as QKD network control and management technologies, and has also conducted field demonstrations. In 2010, Tokyo QKD Network, a test bed constructed in collaboration among industry, academia, and government, recorded the longest operation time in the world, and various demonstrations of principle and practice are being conducted. Regarding implementation, companies in Japan, Europe, and China have commercialized QKD devices. Moreover, telecom carriers and start-up companies around the world have been working toward the commercial provision of services using the QKD network.

For the QKD network technology to spread globally, international standardization is crucial. In collaboration with the government, companies, and universities, NICT is actively working toward international standardization at the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC SC1), European Telecommunications Standards Institute (ETSI), etc. Especially, at ITU-T, Japan is leading the development and publication of many recommendations, including for international standardization of QKD networks.

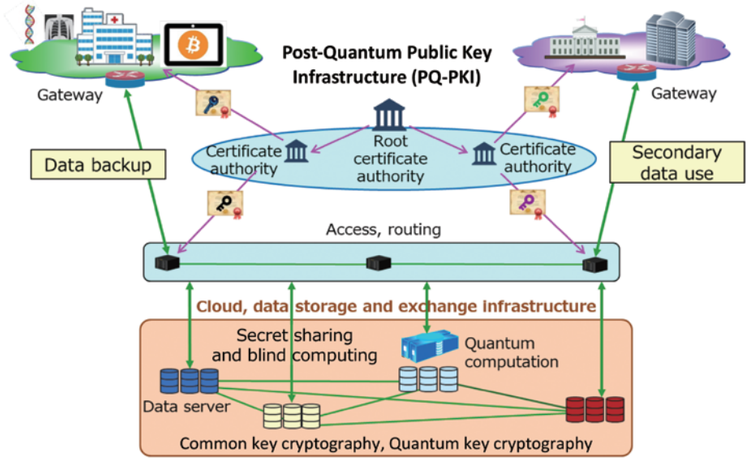

Figure 3 Quantum Secure Cloud Technology

Exploitation of QKD networks and future prospects: Quantum secure cloud technology

To apply the high secrecy of quantum cryptography in society, it is necessary to develop application technologies by taking a broad view of communication systems and security technology as a whole. One of those technologies is quantum secure cloud technology, which is being developed by NICT in collaboration with industry and academia. This enables the storage and computational processing of data backups that cannot be decrypted or tampered with by any computers, by merging authentication infrastructure and blind computing with quantum cryptography, secret sharing, and post-quantum public-key cryptography (Figure 3). By storing data in several servers in a distributed, encrypted form, this technology realizes both information-theoretic security, in which even if the information in some servers is leaked, the original data cannot be restored, and availability, in which if the information in some servers is lost, the original data can be restored from the remaining information at the same time. This proprietary technology was developed in Japan, and NICT and companies are conducting demonstrations of storing important data in various fields including the medical industry. It is expected that a new security infrastructure for the networked society will be developed by properly merging the QKD network with various contemporary security technologies. The NICT Quantum Network White Paper describes the principle of the technology, requirements, and prospects for social implementation in detail.