Quantum Cryptography – the Next Generation of Light-based Cryptographic Technology

ITO Yoichiro, TOYAMA Hiroyuki

Abstract

Quantum cryptography is an encryption method capable of protecting information for a very long period without the risk of being decrypted even far into the future. It is expected to be applied to mission critical systems at the nation level. Quantum cryptography is used to encrypt communications using a technique called a one-time pad, which uses a procedure in which cryptographic keys are produced in advance by quantum key distribution (QKD) for sharing between the parties. QKD enables key information to be placed on photons, which are particles of light, to protect the key with their properties of quantum mechanics. In addition to the method called BB84, NEC is conducting research on the continuous-variable quantum key distribution (CV-QKD) method, a next-generation technology.

Keywords

safe and secure cyberspace, security, quantum key distribution (QKD), quantum cryptography

1. Why Quantum Cryptography Now?

Modern society has greatly benefited from highly advanced information infrastructure, including the Internet. As information becomes more and more indispensable in our society, it is conceivable that the way we live our lives and how our society works would be endangered if information was to be stolen by a malicious third party.

NEC has set safety, security, fairness, and efficiency as the social values required to realize a more prosperous society. This paper introduces quantum cryptography as the ultimate technology to make that dream a reality.

1.1 Safety of modern cryptography

Most of the information exchanged in today's society is protected by modern cryptography that uses the advanced encryption standard (AES), Rivest-Shamir-Adelman (RSA) encryption, and other techniques. Put simply, modern cryptography means that everyone knows the algorithms or encryption methods, but the information is kept secret by concealing the keys. The safety of modern cryptography is secured by the fact that the calculations for breaking the key take an extremely long time.

1.2 Risk of modern cryptography

The security of modern cryptography, however, is going to be threatened by the advent of quantum computers. For example, with RSA encryption, the calculation of the prime factorization of very large numbers takes an extremely long time, but the use of quantum computers is known to do these calculations a short time. Of course, the prime factorization of even larger numbers will still take time to decipher even with the quantum computers currently being developed. This leads only to the repetition of the same old methods. Given that the whole world is engaged in research into quantum computers and that progress has been rapid in recent years, experts fear that modern cryptography will soon be compromised.

1.3 Significance of quantum cryptography

Quantum cryptography can end the repetition mentioned earlier. Even when the most powerful quantum

computer or a future computer boasting unprecedented capabilities is used, quantum cryptography guarantees the impossibility of being deciphered. This absolute safety is the biggest significance of quantum cryptography.

Although quantum cryptography is categorized as symmetric-key cryptography, it has features that are very different from conventional cryptography. Quantum cryptography uses a protocol to ensure that the key is absolutely safe and automatically shared between the sender and receiver, which has long been a concern in the use of cryptography.

2. What is Quantum Cryptography?

This section outlines the reasons for the absolute safety of quantum cryptography.

Quantum cryptography consists of two elements called one-time pad and quantum key distribution (QKD) (**Fig. 1**). The one-time pad is a method of encryption/decryption in actual communications; QKD is a method of transmitting and sharing cryptographic keys in advance.

2.1 One-time pad

With the one-time pad, the sender and receiver share a random number of the same length as the transmitted/received message in advance. They use that random number as the cryptographic key for encrypting/decrypting the message. The key is discarded after every use. The operation used for encryption/decryption is a very simple and lightweight one called XOR.

It was mathematically proven in the 1940s that the one-time pad method of encryption/decryption can never be decrypted. The reason why this method has not been used despite its simplicity and absolute safety was that sharing keys having the same length as the message was not realistic. QKD, which is based on quantum mechanics, has made it possible to compensate for this issue.

2.2 Quantum key distribution (QKD)

QKD is a method that allows the sender and receiver of a message to share a cryptographic key that is a random number in advance.

Here is a simplified explanation for the sake of clarity. One bit of the key's information is assigned to a single photon that is transmitted from the sender to the receiver. If a third party tries to eavesdrop and steal the photon in the middle of transmission, the photon will not reach the receiver, because the photon cannot be split further according to quantum theory. Even if an eavesdropper steals the photon and returns it, the status of the photon will change in accordance with quantum mechanics, and the receiver can detect the eavesdropping. Therefore, by putting key information on a single photon and transmitting/sharing it, eavesdropping can be detected and prevented. In effect, only secure cryptographic keys can be shared, not keys that can be intercepted by an eavesdropper.

Several protocols or methods have been developed for use in QKD, and each method has its own strict safety argument. To prove security, it is assumed that an eavesdropper can physically attack the system in any way. Because its security is theoretically proven, quantum cryptography can be said to be absolutely secure in the future.

2.3 BB84 QKD

This section gives a simplified description of a typical QKD protocol called the BB84 method.

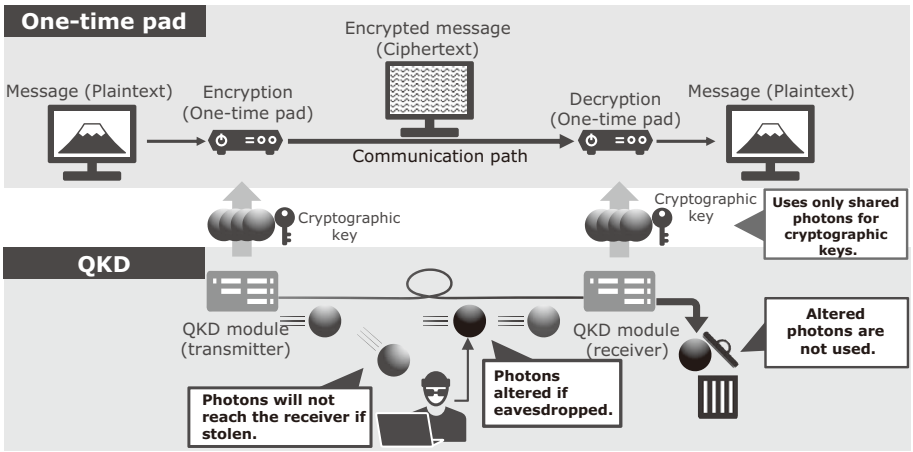

Fig. 1 Outline of how quantum cryptography works.

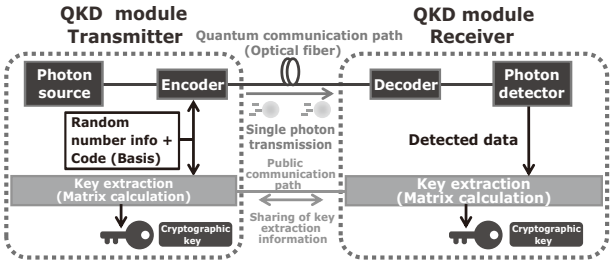

Fig. 2 Outline of BB84 QKD.

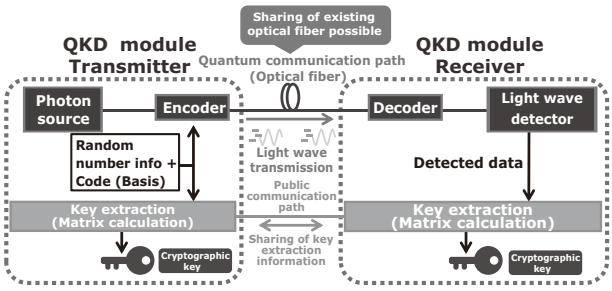

Fig. 3 Outline of CV-QKD.

The sender assigns one bit of the key's information to each of the photons (**Fig. 2**). Specifically, for the transmitter, one bit of information generated from a random number is assigned to each photon as it leaves its source and is sent. The receiver detects the single photon using a photon detector and reads the bit of information. In case of eavesdropping, the attempt can be detected and prevented as described in section 2.2. In real-world implementation, the program to determine eavesdropping and the subsequent key extraction is designed based on a theoretically secure key distribution protocol (Fig. 2).

At present, a protocol called the decoy BB84, which is a slightly more complicated version than the aforementioned BB84 method, has been proven to be absolutely secure and is being developed worldwide. NEC is also conducting research and development (R&D) jointly with the National Institute of Information and Communications Technology (NICT).

2.4 Continuous-variable quantum key distribution (CV-QKD)

This section describes the protocol of the continuous-variable quantum key distribution (CV-QKD) method (**Fig. 3**). Detecting photons used in BB84 requires a high performance photon detector. It also has some limitations, such as that it is necessary to occupy an optical fiber.

With the CV-QKD method, the transmitter sends a single bit of key information to the receiver based on the phase difference between weak light waves and regular light. The receiver does not need to use a light wave detector with a particularly high performance. QKD can consequently coexist with typical optical communications using the same optical fiber and therefore be implemented at a lower cost.

At present, NEC is conducting R&D of this method in collaboration with Gakushuin University.

2.5 Issues in QKD and countermeasures

QKD also has its own issues, or rather physical limitations. Transmitting a single photon over an optical fiber results in a large losses in transmission. This puts a constraint on the distance and the key generation speed that is how many bits of cryptographic key can be generated per second. With the device developed at NEC, the transmission distance is about 50 kbps to 100 kbps at 50 km.

The distance constraint can overcome by connecting QKD modules and using key relays. In fact, the possibility of a key relay has already been tested and demonstrated by the Tokyo QKD Network run by NICT.

The constraint of the speed at which keys are generated can be solved by using a method called wavelength multiplexing to increase the amount of keys generated or by combining QKD with another modern cryptography method such as AES to obtain a balance while key sharing. These countermeasures have already been demonstrated at NEC.

3. NEC's Research and Development Status

NEC is engaged in a variety of R&D activities aimed at the commercialization of QKD. NEC believes that it is necessary to maintain a stable key supply for a long period under severe conditions in the field so that QKD can be applied to the real world.

In particular, NEC's BB84 system has circuitry with a PLC interferometer that has a high resistance even when used with optical fibers that have external environmental fluctuations. NEC has demonstrated long-term stable operations in severe environments (**Fig. 4**).

Fig. 4 External view of NEC's BB84 system prototype.

4. Social Implementation

NEC is conducting various practical experiments for the social implementation of quantum cryptography. In this section, the approach and efforts made by NEC are introduced.

4.1 Practical experiments in the biometrics field*

Biometric authentication identifies people by extracting their physical features. Some of its advantages are that it is easy to use and the identifiers cannot be lost. On the other hand, there is also an issue of the impossibility of updating information if it is stolen. In addition, the reference data for biometric authentication is personal information, which must be securely protected.

NEC collaborated with NICT to develop a system that integrates quantum cryptography and biometrics to conceal the feature data transmitted when facial recognition is used. The system has been demonstrated on the Tokyo QKD Network (**Fig. 5**).

4.2 Practical experiments in the medical field*

In recent years, natural disasters have been causing increasingly severe damage, but medical services must be maintained even in the case of disaster. This makes it necessary to create a system that can store patients' electronic medical records at remote locations where the data can be recovered and retrieved in the event of a disaster.

NEC in collaboration with NICT and ZenmuTech, Inc. solved this issue by developing a system that uses quantum cryptography to encrypt the electronic medical records and transmit the information securely through a network (**Fig. 6**).

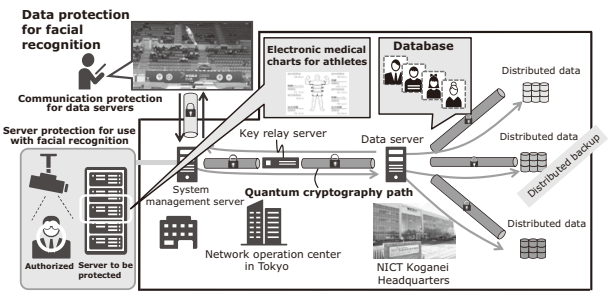

Fig. 5 Outline of practical experiments using facial recognition.

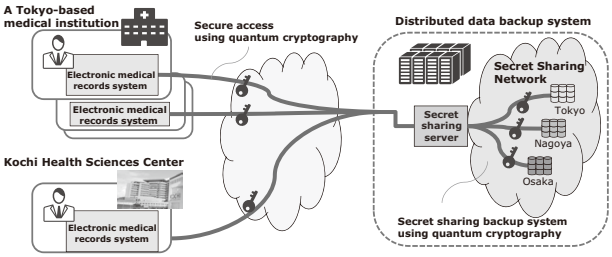

Fig. 6 Outline of practical experiments in the medical field.

4.3 Plan for practical experiments in the financial field*

Increasing threats of cyberattacks on financial organizations are leading to concerns about the impact on financial systems. Against this backdrop as well as the publication of the Financial Field Cybersecurity Report requesting the enhancement of countermeasures, it has become urgent to take new safety measures to prepare for future threats.

NEC is planning to verify the applicability of quantum cryptography to the financial field in collaboration with Nomura Holdings, Inc.; Nomura Securities, Co., Ltd.; NICT, and Toshiba Corporation.

5. Future Outlook

Digital transformations that make use of data are expected to accelerate in the future. In a world where data is the source of various social values, it is also essential to have a method to securely protect the data and the new values created. NEC aims to provide total solutions, including quantum cryptography, to create a prosperous society supported by safety and security in the next generation.

In closing, note that NEC's quantum cryptographic research activities are based on the results of national projects (NPs) such as the Impulsing Paradigm Change through Disruptive Technologies Program (ImPACT) and the second phase of the Cross-ministerial Strategic Innovation Promotion Program (SIP).

* The practical experiments described in sections 4.1 to 4.3 were performed for Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Photonics and Quantum Technology for Society 5.0" (Funding agency: QST).

Authors' Profiles

ITO Yoichiro
Manager
National Security Solutions Division

TOYAMA Hiroyuki
National Security Solutions Division

The details about this paper can be seen at the following.

Related URL:

Communication Theory of Secrecy Systems
http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf

The Tokyo QKD Network
http://www.tokyoqkd.jp/

High-security, high-availability transmission and storage of biometric data is achieved using quantum cryptography (Japanese)
https://jpn.nec.com/press/201910/20191029_02.html

NEC, NICT and ZenmuTech use quantum cryptography to encrypt, transmit and backup electronic medical records
https://www.nec.com/en/press/202010/global_20201022_01.html

Beginning Joint Verification Tests on Quantum Cryptography Technology to Enhance Cybersecurity in the Financial Sector
https://www.nec.com/en/press/202012/global_20201221_01.html

Update of the Policy Approaches to Strengthen Cyber Security in the Financial Sector
https://www.fsa.go.jp/en/news/2019/20190115.html

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese English

Vol.16 No.1 Social Infrastructure that Guarantees Safety, Security, Fairness, and Efficiency

Vol.16 No.1
October 2021

Special Issue TOP

Papers for Special Issue

NEC Information