3 Quantum Key Distribution Network
3-1 Research and Development of Quantum Key Distribution Network in NICT

Mikio FUJIWARA and Masahide SASAKI

We report a quantum key distribution (QKD) system which enables us to communicate with information theoretical security. The security of the QKD is guaranteed by the low of physics. Basically, the QKD links provides point-to-point secure communication. However, we can extend application/service ranges by constructing a QKD network. NICT has developed the QKD network architecture which has a centralized control structure. In this paper, we introduce the QKD principle, QKD hardware, and the network architecture.

1 Introduction

The concept that everyone can access information, so-called "Big Data," via the internet to which PCs, home electric appliances, automobiles, robots smart meters etc. are connected, that is, IoT (Internet of Things), has been spreading very quickly these days. In the society where real space and cyberspace sophisticatedly merge through IoT, we have convenience, but at the same time, attackers can easily execute attacks in cyberspace using malicious software (so-called "malware"). Actually, methods of high-level and systematic attack that are suspected to be from national entities emerged and became a cause of serious damage to life, economy and social activities. The threat to the security of our country has been increasing year by year. Public key encryption or common key encryption that we use for network services to guarantee security are based on difficult mathematical problems. The risk of safety of such mathematical cryptography increases as calculation technology progresses. Especially, once an encryption key is broken, the safety of all functions of encryption based on it collapses. For example, the safety of RSA cryptography that is the most typically used public key cryptography is based on the difficulty of the prime decomposition problem. Now, the specification of a 1,024-bit key length is at risk of being decrypted. Therefore, the system is undergoing a shift to a 2,048-bit key length [1]. Here, we have to pay attention to the fact that updating a cryptography system forces increased hardware load. For example, comparing 1,024 bits with 2,048 bits, the throughput of 2,048 bits uses 5-30 times more load than that of 1,024 bits. This may degrade performance for the user. Also, even if the upgrade to 2,048 bits is accomplished, the cryptography system would cease to be useful when new mathematical knowledge concerning decrypting of the cryptography algorithm is discovered. The possibility of using a cryptography system that has been broken is not zero as the worst case.

Also, an eavesdropper (usually named Eve) may duplicate and save the data transmitted via a channel even though she cannot decrypt it now but may decrypt it in the future when she acquires the key used for the cryptography system by chance or acquires a new decryption technology that enables decryption. For example, Edward Snowden disclosed the fact in his so-called "Snowden Files" that the intelligence agencies in the United States record encrypted data on internet in order that they will be able to decrypt them in the future. Actually, it is well known that intelligence agencies in the United States and Europe have performed wiretapping on a large scale and for a long time via optical fiber networks (The Guardian, Washington Post, 2013). The technology used for the purpose was a tapping device that is used for diagnosis of optical switches or optical fiber. These days, small commercial tapping devices are sold that can be used as optical wiretapping devices. It is needless to use special tapping devices for wiretapping because most advanced optical detectors can reveal signals inside optical fibers [2]. This is the so-called "crosstalk" phenomenon between optical fibers, in which optical signals leak easily between adjacent optical

fibers in cable when the cable is bent. These facts strongly suggest the necessity of cryptography technology that has the so-called "forward secrecy" to ensure confidentiality in the future.

In order to cope with these clear and present dangers, quantum key distribution (Quantum Key Distribution: QK) is the method to share an encryption key with distant two places, which will theoretically not allow any information to be leaked to any other third party (eavesdropper) by any method. This method, called the BB84 protocol, was proposed by Bennett (C. H. Bennett) and Brassard (G. Brassard) in 1984 [3]. It had not so much attracted attention for about ten years since the proposal. However, as quantum calculation algorithms that efficiently solve prime decomposition problems or discrete logarithm problems were discovered in 1994 [2], and new threats against key exchange systems or cryptography systems that are used on the internet emerged, the BB84 protocol suddenly came into the spotlight.

The security of QKD does not depend on difficult mathematical problems but is based on universal physical laws of quantum mechanics. In the method of QKD, information expressed by a random number sequence of 1s and 0s is coded to signals of which quantum mechanical property is properly controlled for transmission. A safe random number sequence that is free from the anxiety of eavesdropping can be shared by excluding bit data that may have the possibility of being eavesdropped from shared random numbers, by using the no-cloning theorem where the quantum state cannot be copied (copying is impossible) without error and the characteristic that measurement in the transmission route (so-called "eavesdropping") always leaves traces in such signal condition (uncertainty principle). Actually, "the amount of leak of information to eavesdroppers can be reduced by appropriate signal processing (key distillation processing) even if QKD communication is eavesdropped with any technology that is permissible by physical law." This can be proved by the information theory method. It is said that QKD represents "unconditionally secure" distribution of the key, which implies that there is no assumption of the ability of eavesdroppers. Encrypted communication that no computer of any ability nor future technology can decrypt will be realized by sending cryptographic keys thus shared by proportionate preparation with the data size of the plaintext bit to be transmitted, by generating a cryptogram from the plaintext bit data and XOR, and not using the same cryptographic key more than once (so-called "Vernam's one-time pad" (OTP)).

Many organizations have performed research and development on this until today. Many protocols other than the BB84 protocol have been invented one after another [4][5], and security proof and theory analysis methods have been developed and performance of instruments have improved. Several venture companies started in Europe and the USA since the latter half of 2000 succeeded in commercialization of QKD devices [6]-[8]. In 2005, a project (The DARPA Quantum Network) supported by the US Defense Advanced Research Projects Agency constructed an urban-area QKD network in Boston in 2005. The key generating rate of a ring network connecting 3 points was about 1,000 (1 k bits per second:1 kbps for about 10 km optical fiber [9]. In 2008, a research project in Europe, SECOQC (Secure Communication based on Quantum Cryptography), constructed an urban-area QKD network that connects 6 points in Vienna. They succeeded in demonstrating and verifying interconnection of QKD devices of several methods. The typical key generation rate was 1 kbps for about 30 km of embedded optical fiber. Encrypted communication of voice was verified [10]. Since the success of SECOQC, the Europe Telecommunication Standardize Institute started to standardize QKD [11].

In Japan, an industry-academia-government collaboration project promoted by the Ministry of Internal Affairs and Communications and NICT started in 2001, by which the key generation rate of QKD device improved 100 times. In 2010, the industry-academia-government team constructed a test bed "Tokyo QKD Network," a key exchange network consisting of 6 nodes in the Tokyo area, and succeeded for the first time in the world the confidential transmission of video [12].

From FY2011 to FY2015, NICT researched and developed test operation of a QKD system and safety evaluation technology under the project of "research and development of secure photonic network technology" (No. 157) funded for the 5 years [13]. Also, a new application that uses a cryptography key supplied by a QKD network has been developed and an application interface for various communication devices such as network switches [14] [15], smartphones [16] and drones [17] [18] has been developed. A network solution that has various interfaces other than a key distribution function and a key management function is called a QKD platform and it is already being test-operated on the Tokyo QKD Network. It enables exchanging cryptography keys that cannot be eavesdropped or decrypted by a computer of any ability or any future technology between various information communication terminals,

that can reinforce the security of the whole system, by introducing a QKD platform suitable for needs such as black box and installing the application interface in information devices even though users do not know the details of it.

In 2015, a practical use level verification test started, by transferring the QKD devices that passed verification tests under the condition of test bed. For example, Nippon Electric Company, Limited (NEC) has performed a verification test for cryptographic communication of cyber threat information at the hub a "cyber security factory" somewhere in Tokyo since July 2015 [19]. It continued until the end of FY2016. Since then, the subsequent research and development has been performed by the quantum secure photonic network team.

Toshiba has been performing a cryptography communication experiment of genome analysis data using a 7-km circuit line between the Toshiba life science analysis center in Sendai city and the Tohoku University Tohoku Medical Megabank Organization since August 2015 [20] until August 2017. The key generation rate of these QKD devices is more than 50 times faster than that of products of venture companies abroad. The rate is about 1 Mbps for a transmission distance of 50 km using standard optical fiber with an optical loss rate of 0.2 dB/km, and about several hundred kbps for transmission distance of 50 km using commercial optical fiber (which averaged an optical loss rate of about 0.5 dB/km) actually constructed in the Tokyo area. On the other hand, these days, a national project lead by the University of Science and Technology of China is accomplishing infrastructure of nationwide super-highly-confidential communication by constructing urban area QKD networks with 50 nodes in Beijing, Jinan, Hefei and Shanghai and constructing a QKD backbone of total length of 2000 km with 32 relay nodes [21]. Also, in the USA, Battelle announced that they had a plan to establish an inter-city QKD network of 700 km in collaboration with a venture company from Switzerland, id Quantique, and to release as open test bed for nonprofit organizations [22].

Thus, the technology of QKD has progressed to the stage of test operation under the realistic condition of urban areas or among cities. In the future, it will be necessary to improve the technology so as to construct a super-confidential communication infrastructure by strengthening its practicability by stimulating operational experiences of a QKD platform under realistic condition and knowledge on safety evaluation. In this article, I provide a rough outline of QKD and introduce the QKD network architecture for which NICT is leading the development.

2 Principle of QKD operation

2.1 QKD protocol and its principle

In QKD, a transmitter encodes bit information of a random number sequence of 1s and 0s to appropriate quantum signals for transmission, and a receiver receives

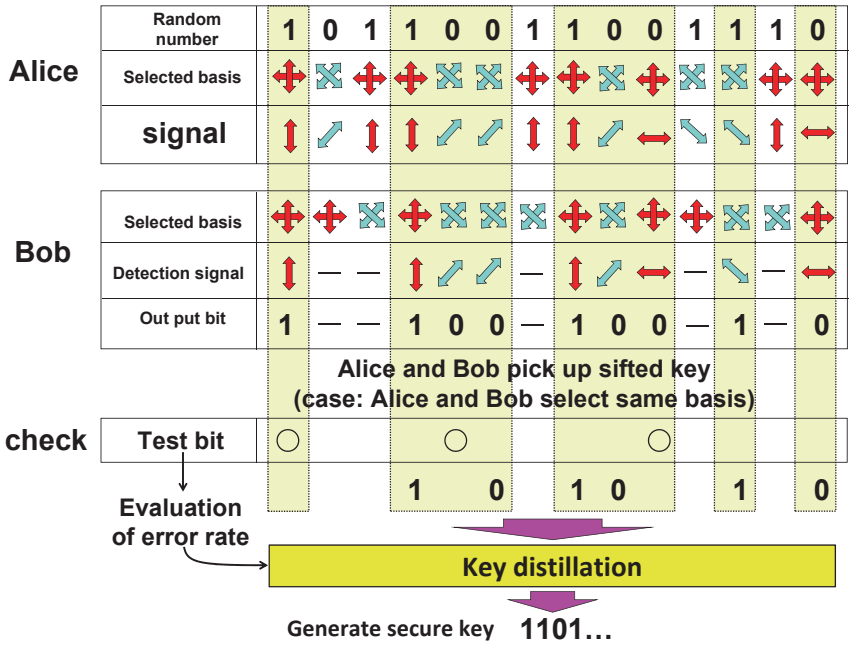

Fig. 1 Outline of the BB84 protocol using polarization (corresponding table on bit information and base information between transmitter and receiver)

quantum signals by using an appropriate measuring method. Quantum signals must contain at least more than two non-orthogonal states. Hereafter in this article, I explain the representative QKD protocol of BB84 as an example. The outline of the protocol is shown in Fig. 1. In the field of cryptography, traditionally, we call the authorized transmitter Alice and the authorized receiver Bob and the eavesdropper Eve. Hereafter, I follow this tradition. Also, in the outline of the BB84 protocol, the case that the polarization state of a single photon as a quantum signal is used as an example.

In the BB84 protocol, two sets of polarization states, that is, the Z-base of horizontal and vertical polarization {|H>, |V>}, and the X-base of dextrorotation and levorotation polarization {|45°>, |−45°>} are used. {|H>, |V>} is expressed as {|Z0>, |Z1>}, and {|45°>, |−45°>} is expressed as {|X0>, |X1>} to describe the protocol. The transmitter (Alice) encodes 1s and 0s to the corresponding polarization state selecting one of the two from the Z-base and the X-base when she encodes each bit of information of 1s and 0s of a random number sequence to a photon. Therefore, the quantum signal to be transmitted consist of four components of {|Z0>, |Z1>, |X0>, |X1>}. Though the state vector in each base crosses the other orthogonally, the state vectors between the Z and X bases do not cross orthogonally. In reality, the inner products are as follows.

$$\langle Z0|X0\rangle = \langle Z0|X1\rangle = \frac{1}{\sqrt{2}} \tag{1}$$

$$\langle Z1|X0\rangle = \langle Z1|X1\rangle = \frac{1}{\sqrt{2}} \tag{2}$$

Figure 2 shows a simple example of a correspondence table of bit information and base information used between the transmitter and receiver.

The receiver (Bob) selects one from the Z-base or X-base at random and independently from the transmitter to measure photons. Sometimes no photon is detected due to optical loss in the quantum communication channel. There is some noise in the quantum communication channel so that the state detected is different from that of transmission. Such case is not shown in Fig. 1.

After transmission of this quantum signals, Alice and Bob do not disclose the bit information but exchange only the information on the base they actually used (base information) via a public transmission channel, and select the slot where the bases of Alice and Bob coincide (base comparison). The bit sequence thus remaining is called the sieving key. Then, a part of the sieving key is selected as a test bit for comparison between Alice and Bob to evaluate the bit error rate.

If eavesdropping exists in a quantum transmission channel, the bit error rate increases. That is because the sequence retransmitted to Bob always generates errors due to the non-discriminability theorem or impossibility of duplication even if Eve tries to copy the sequence of non-orthogonal states in a quantum transmission channel by

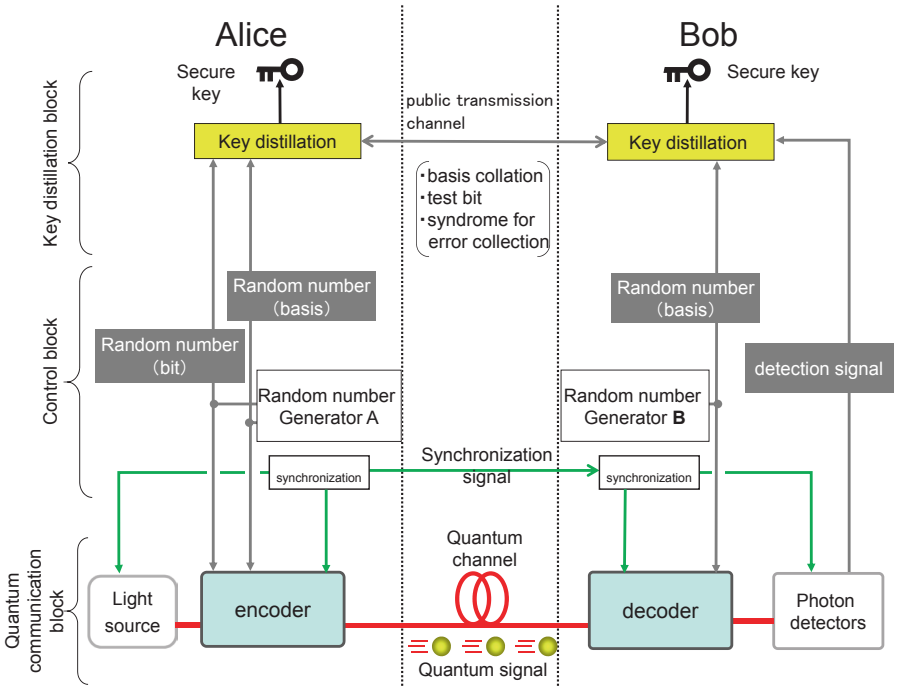

Fig. 2 Block diagram of QKD link

contriving an eavesdropping method. Alice and Bob can discover eavesdropping by comparing test bits randomly selected from the sieving key.

Even if Eve does not exist, the bit error rate will increase when there is noise in a quantum transmission channel. As there is no method to distinguish if the noise is caused by Eve or not, all noise in the quantum transmission is assumed to be an effect caused by Eve.

Alice and Bob judge the possibility of eavesdropping from the bit error rate of the test bit. If they judge that there is no possibility of eavesdropping, they extract an ultimately safe random number sequence by processing appropriate key distillation according to the value of the bit error rate to extract a cryptographic key.

2.2 Composition of QKD link

A QKD link consists of a "quantum communication block" for sharing random number data via photons, a "key distillation block" for extracting safe cryptography key from shared random number data, and a "control block" that controls these blocks. The control block supplies a random number sequence to the quantum communication block and the key distillation block also supplies a synchronous signal to the quantum communication block for time synchronization. The rough system structure is shown in Fig. 2. In most cases, Alice multiplexes the synchronous signals with quantum signals physically and transmits them to Bob via a quantum communication channel. In the following, details of the quantum communication block and the key distillation block are explained.

・Quantum communication block

The quantum communication block consists of a light source, encoder, quantum communication channel, decrypter and photon detector. It transmits quantum signals by synchronizing time via synchronous signals.

A laser light source is often used as a light source rather than a single photon source. Actually, long-distance QKD can be realized with laser light pulses by controlling as follows. First of all, the following four procedures should be performed.

(i) Weak laser light: attenuating laser light to a weak pulse with a probability of containing two or more photons per pulse to introduce the light into the communication channel.

(ii) Phase disordering: controlling the light source or modulator in order to generate phase-uncorrelated bit strings.

(iii) Decoy method: introducing pulses of different laser light intensity other than the signal pulse used for key generation (decoy pulse) randomly in order to prevent degradation of transmission performance due to several photon components not being removed.

(iv) Time-bin signal: generating two pulse pair (time-bin) [23] and coding bit information and base information to the pair.

(i) is a requirement to generate a state of which the main component is a single photon.(ii) and (iii) are requirements to strengthen transmission performance. (iv) is a requirement to be considered for the case of an optical fiber quantum transmission channel. Time-bin signal can suppress the effect of perturbation generated in an optical fiber more effectively than polarization signal. Actually, the effect of perturbation can be eliminated by detecting photons by having two pulses by a receiver interfere because the two pulses are perturbed almost at the same time. This is explained in the following by an example of the composition of encoder devices in practical use for these points (Fig. 3).

Laser light can be attenuated by an attenuator just before the exit of the encoder. Hence, the requirement (i) "weak laser light" is performed at the last step in the encoder. Before the step, laser light with sufficient intensity (classic signal) is coded. Although the laser is in coherent state of the same phase, correlation between input pulses must be eliminated in order to improve the transmission performance of the BB84 protocol. (requirement (ii) "phase disordering").

If there is a phase correlation between pulses, Eve presumes the phase from the pulse sequence and can perform quantum measurement so as to compensate the effects by the Decoy method. Therefore, this situation will deteriorate the safety. In the example of implementation of a typical high-speed QKD device, a laser light pulse without such phase correlation is generated by a repeat rate of 1.244 GHz. The time interval is about 50 picoseconds (5×10^{-12} sec, 50 ps). The laser light pulses are input into the encoder one after another with an interval of 800 ps. This pulse sequence is defined as $|\alpha 1\rangle$, $|\alpha 2\rangle$, $\alpha 3\rangle$, ···, Here, the amplitude is expressed as $\alpha 1 = |\alpha|e^{i\theta 1}$, $\alpha 2 = |\alpha|e^{i\theta 2}$, $\alpha 3 = |\alpha|e^{i\theta 3}$, ···, phases$\theta_1$, θ_2, θ_3,··· must change randomly without correlation each other. In this subsection, I explain how the laser light pulses of a certain phase are input to an encoder and are output as "time-bin signals" that meet the requirement (iv) with which bit information and base information are coded.

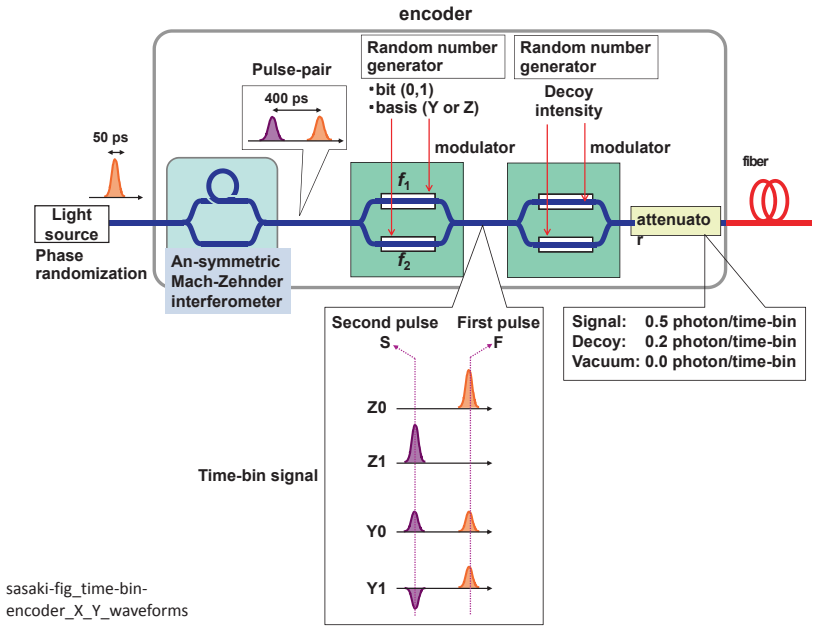

Fig. 3 Composition of encoder used for device implementation of the BB84 protocol for optical fiber transmission and outline of time-bin signal

Laser light pulses can be modulated to pulse pair with 400 ps delay by going through two light paths of different lengths and by multiplexing them (by going through asymmetric interferometer). This pulse pair is expressed as $|\alpha\rangle_F \otimes |\alpha\rangle_S$. Here, suffixes F and S mean temporally first pulse (First) and the second pulse (Second) that imply the positions of pulses, respectively. Then, the pulse pair are input to a dual drive optical modulator with two electrodes. Then, the two pulses are multiplexed after modulated with phases φ1 and φ2 that correspond to bit information and base information at each electrode, according to the random number sequence applied by random number source A of the control block shown in Fig. 2. The states are described by the following equations.

$$|\Psi_{Z0}\rangle = |\alpha\rangle_F \otimes |0\rangle_S \tag{3}$$

$$|\Psi_{Z1}\rangle = |0\rangle_F \otimes |\alpha\rangle_S \tag{4}$$

$$|\Psi_{Y0}\rangle = \left|\frac{\alpha e^{-i\pi/4}}{\sqrt{2}}\right\rangle_F \otimes \left|\frac{\alpha e^{i\pi/4}}{\sqrt{2}}\right\rangle_S \tag{5}$$

$$|\Psi_{Y0}\rangle = \left|\frac{\alpha e^{i\pi/4}}{\sqrt{2}}\right\rangle_F \otimes \left|\frac{\alpha e^{-i\pi/4}}{\sqrt{2}}\right\rangle_S \tag{6}$$

Here, $|\Psi_{Z0}\rangle$ and $|\Psi_{Z1}\rangle$ the states correspond to the Z-bases, and $|\Psi_{Y0}\rangle$ and $|\Psi_{Y1}\rangle$ are the states corresponding to the Y-base. These four states have equivalent effect concerning the Z-base, X-base and the function of QKD of the polarization mode explained above. Here, the reason for using Y for the base is only for convenience because we use input power for the modulator.

After that, the time-bin signals are input to the second dual drive optical modulator. Then, the signals are modulated randomly into several types of intensity according to the requirement (iii) "Decoy method" and pass through the attenuator to become a weak optical pulse. Lastly, it is input into the optical fiber of quantum communication channel. One of the examples of the Decoy method is the two settings of signal intensity $|\alpha|^2$ = 0.5 photon/time-bin, decoy intensity $|\alpha|^2$ = 0.2 photons/time-bin, and $|\alpha|^2$ = 0 photon/time-bin (vacuum). It is not possible for real laser light to decrease the probability that two or more photons are contained in a pulse to zero. Hence, the state with two or more photons in the time-bin pulse still remains. In such a case, a so-called "photon number splitting attack" is possible for Eve by stealing a photon and transmitting the others photons to Bob keeping the states.

In this case, a bit error never occurs because the base and contents of the bit do not change. Therefore, the eavesdropping cannot be detected. The Decoy method can improve tolerance to such an attack and can extend transmission distance. If the photon distribution of the light source is known, the detection rate and error rate of signal are determined by the loss of the transmission channel. However, if there is an attack in which a multi-photon state

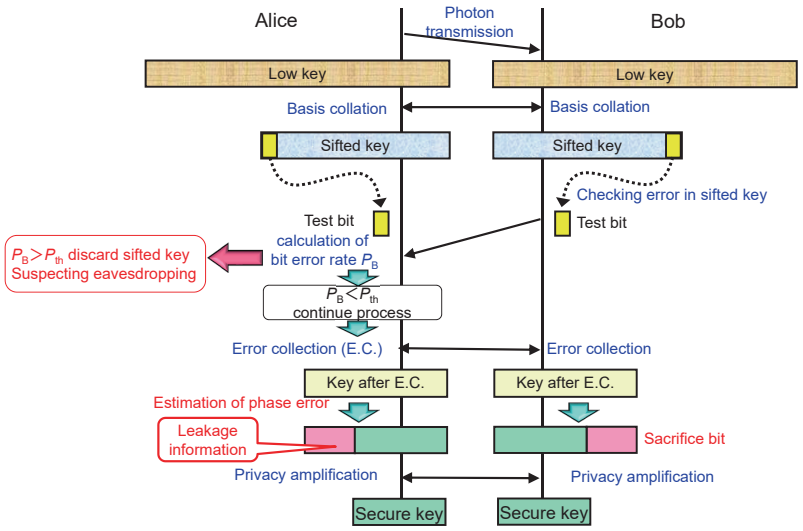

Fig. 4 Flow of key distillation process

is picked up, the rate changes and the amount of information leaked to eavesdropper can be estimated. For more details see [24] and [25].

・Key distillation block

The key distillation block consists of a key distillation device of the receiver and a public communication channel for connection. The random number sequence sources of control block A and B supply the same random number sequence to the encoder and decrypter to the key distillation device. Also, the detection signal from the photon detector is supplied to Bob's key distillation device via control block. The data comparing the detection signal of Bob and its corresponding random number sequence data is called the "raw key." Time synchronizing is performed using a synchronous signal for exchanging random number sequence and detection signals. The raw key thus shared is processed for key distillation described as follows to extract the ultimate cryptography key.

Figure 4 shows a rough flow of the key distillation process (conforming to the BB84 protocol as an example). After transmission of a photon, numerous data on the raw key data are created at Alice and Bob. The data is grouped in as large blocks as possible, for example one million bits, and the key is distillated by the blocks as is shown in Fig. 4.

(i) For the first, comparing the base via public communication channel and extracting the bit sequence of the same base as the "sifted key"

(ii) Picking up a part of the sifted key as a test bit and sharing it between the transmitter and receiver via public communication channel, and then calculating the rate of different bits of the Z-base, the so-called "bit error rate PB"

(iii) If this value is larger than a certain threshold P_{th}, ($PB \geq P_{th}$), it is judged as a eavesdropping and key distillation is stopped by discarding the whole block.

(iv) If the value is smaller than the threshold ($PB < P_{th}$), an error correction process is applied to the sifted key.

(v) Moreover, estimating the phase error rate and deciding the rate of "sacrificed bits" according to the phase error rate, and extracting an ultimate safe cryptography key by performing confidentiality enforcement processing according to the rate

Even when Eve eavesdrops, if the bit error rate is smaller than the threshold ($PB < P_{th}$), it is possible to suppress the amount of information leaked to Eve to effectively zero by discarding some amount of bits randomly selected from the "error corrected key" of which confidentiality is strengthened as "sacrificed bits."

For example, in the case of the standard BB84 protocol, the threshold is about P_{th} ~11 %.

In reality, bit errors in QKD can be caused by transmission errors in the quantum communication channel, device errors at modulation and demodulation and noise of the photon detector in addition to eavesdropping. As it is impossible to distinguish a bit error due to incompleteness of devices from that by eavesdropping, the worst condition for transmitters and receivers, it is assumed that all errors are caused by the eavesdropper.

The most advanced QKD device can suppress the bit error rate P_{th} to several % through several 10 km field installed fibers. If the bit error rate increases from this value, it is determined that eavesdropping occurred. By the conventional optical communication diagnosis technology, the attack where a photon is picked up for measuring from

the communication channel and is retransmitted by recovering it in the channel cannot be detected but a QKD device can detect such a sophisticated intermediate attack.

Moreover, any eavesdropping attack that leads to leakage of information from an optical communication channel can be detected even if such eavesdropping attack becomes more sophisticated in the future. This is a merit that conventional cryptography technology did not have and is a very important feature for coping with the realization of eavesdropping of optical communication infrastructure. On the other hand, in order to guarantee unconditional safety, some communication performance such as distance and speed may be sacrificed. The performance of the QKD link has a cryptography generation rate of 200,000-300,000 bits (200-300 kbps) through field installed fiber of 50 km.

That means that the speed for cryptography of a one-time pad in real time is capable of an MPEG-4 video at most. On the contrary, the performance of commercial devices by Europe, the US and China is worse than that, about 1 kbps in an urban area.

3 QKD platform

Although there are still upper limits in the distance and speed of direct transmission of QKD, "key capsule relay (key relay)" via "reliable node (trusted node)" enables a wide field and secure key exchange by networking QKD. The system connecting multiple QKD links for networking and implementing key management function necessary for key capsule relay is generally called a "QKD network."

The cost to construct a QKD network is still high, but a generated cryptography key can be distributed to various communication devices and control apparatuses to strengthen security by controlling and managing the key properly. Also, if a large-size key is prepared, cryptography can be largely simplified because encoding is only a "simple" logical sum of the plaintext and key. Hence, the problem of delay of processing is almost resolved and a cryptography method for communication devices becomes easy to unite. So, it will be possible to ensure compatibility in cryptography between organizations of different specifications or methods of security systems by managing key ID properly and relaying key data. Actually, in a special and important communication purpose, an exclusive cryptography network system independent from the open internet is used and its specifications for cryptography are mostly closed. So, it is forbidden to connect between concerned organizations and difficult to interact with each other, which is a basic problem. The introduction of QKD networks will solve such problems and it is expected to be effective to improve interconnectivity.

The system of network solution that users can use as a black box, implementing efficient key management function necessary for realization of such new added value and an interface to support various applications on a QKD network is called a "QKD platform" here. As shown in Fig. 5, it consists of three layers of a quantum layer, a key management layer, and a key supply layer.

In the quantum layer, the cryptographic key is distributed by QKD. QKD itself is done one-by-one via an optical communication channel such as optical fiber or optical space communication.

A network is realized by setting reliable nodes and connecting terminals of QKD links to make a capsule of the cryptographic key from a QKD link by the other cryptographic key of the other link (exclusive logical sum of bits of the key) and relaying them one by one. This key relay is done in the key management layer. That is, the cryptography key generated in each QKD link is managed and operated in the key management layer. In the key management layer, there is a key management agent (KMA) device in each node. The device realizes safe key relay by combining authorization technology not to relay the cryptographic key to anyone other than the legitimate user. The Wegman-Carter authentication method based on information theoretical safety, not on computation amount, is used [26].

The key management server (KMS) also manages the condition of creation of cryptographic keys, the condition of consumption, and the existence of eavesdropping intensively and switches the route in the case of an eavesdropping attack.

Generally, the specifications for requirement and acceptance work are different from the application or devices for installation. In order to supply cryptographic keys to various applications freely, a key supply agent (KSA) is defined in the key management agent, and the necessary application interface is implemented. This layer of a key supplying agent is called the key supply layer. By defining the key supplying layer, the work of interface design by a key supply vendor and a key receiving client and the responsibility of each work can be clarified. Physically, both the KMA and KSA are implemented in the same device (such as a PC), so the key management layer and key supply layer are degenerated.

Thus, the QKD platform consists of a quantum layer

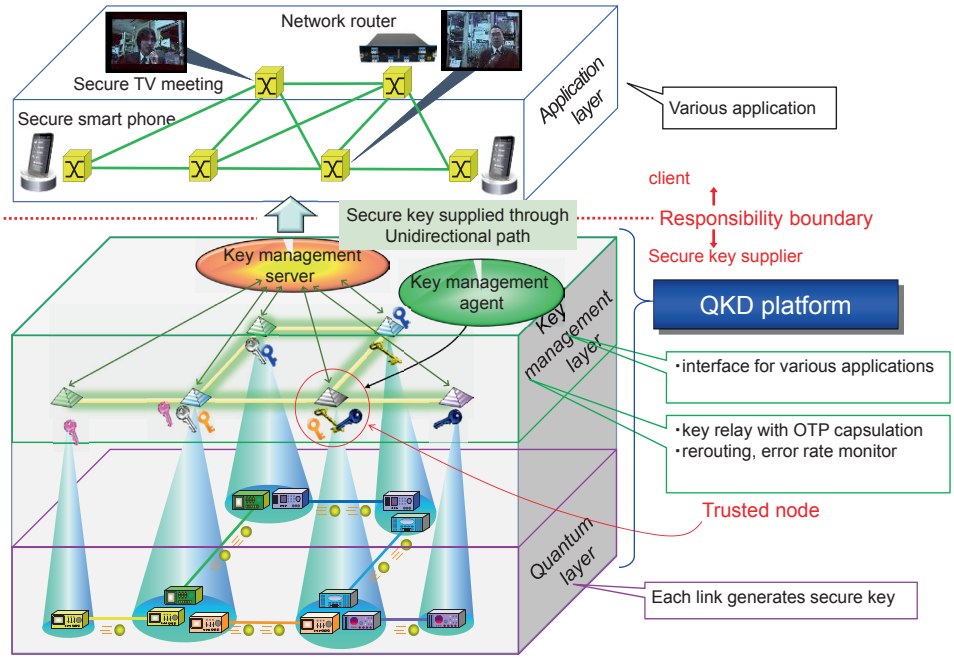

Fig. 5 Concept of QKD platform. It consists of a quantum layer of QKD, a key management layer for management and operation of cryptographic keys, and a key supplying layer on which the application interface is implemented. KMS: Key management server, KMA: Key management agent, KSA: Key supplying agent

for QKD, a key management layer for management and operation of cryptographic keys, and a key supplying layer on which the application interface is implemented.

Strengthening security can be realized by introducing this to an existing network, the existing security functions can be maintained and the security of various applications can be strengthened using cryptographic keys that have forward secrecy. The application layer shown in Fig. 5 is a general term of protocols that use cryptography keys for elucidation of the QKD platform. Hence, its meaning is different from that of "application layer" used for the seventh layer in "OSI (Open Systems Interconnection) reference model" that is widely used in network design. All of the applications to which cryptographic keys are supplied from the QKD platform in any layer of the OSI model are included together into the application layer in Fig. 4.

The user (client) of the application layer obtains cryptographic keys of the necessary amount by informing the QKD platform about the person with whom the user wants to share the cryptographic keys. The QKD platform supplies a cryptography key with forward secrecy in a fixed format based on the requirement. A cryptographic key once supplied by the QKD platform is used at the responsibility of the user.

Thus, the boundary of responsibility is in between the QKD platform and the application layer. On this border, it

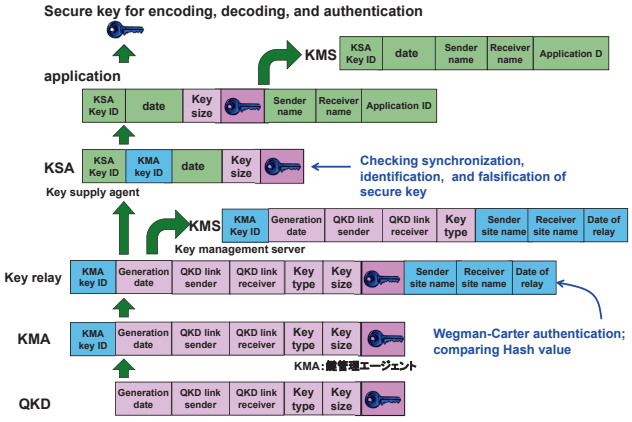

Fig. 6 Outline of key management on QKD platform

is important to supply and receive cryptographic keys using a common interface. By this system, the developer of the application can receive a key by only developing a key receiving client that corresponds to the common interface and he does not need to know the details of the process in the QKD platform. On the other hand, the user of the application layer has management responsibility after receiving the key. On the contrary, those of the QKD platform do not need to know the contents of the application.

If there occurs an unexpected situation or a suspicious incident such as leak of a cryptographic key due to human error somewhere in the application layer, the user discards

the block of the saved cryptographic key and receive a new cryptographic key from the QKD platform to maintain robust security on the network. The data format for key management (outline) used in the key management layer of the QKD platform is shown in Fig. 6.

4 Summary

The principles of a QKD link and a QKD platform that enables operation of a QKD network are introduced in this article. These technologies enable improvement of the safety of transmission channels and storage of data such as genomic data that require safety for a very long term by collaboration with present cryptography technology such as secret sharing [27]. Each country still continues to research energetically in the theory and technology of QKD and the barrier to pay cost in protecting important information is disappearing. NICT will continue to make efforts in improving the technology level in this field so as to maintain and develop technology of the best performance in the world and to offer solutions that ensure safe communication even if technology for decrypting cryptography suddenly appears.

Acknowledgments

The outcomes described in this article were mainly achieved from NICT contract research in "Research and development on secure photonic network technology" (No.157) implemented from FY2011to FY2015 and the ImPACT project "quantum secure photonic network." Hence, the results are the fruits of efforts made by all of the members of quantum ICT advanced technology center and who participated in the projects. I truly thank them for their collaboration in the research and development. I also thank the members of the JGN, Information and Communication System Laboratory, and Security Fundamentals Laboratory for their kind support.

References

1 Recommendation for Key Management: Part 1: General. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57 part1 rev3 general.pdf.

2 M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, "Photon level crosstalk between parallel fibers installed in urban area," Opt. Express, 18(21) 22199–22207, 2010.

3 C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin. Tossing," In Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pp.175–179. IEEE, New York, 1984.

4 N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. 74(1), pp.145–195 2002.

5 V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, and M. P. Norbert Lütkenhaus, "The Security of Practical Quantum Key Distribution," Review of Modern Physics 81:1301–1353 2009.

6 id Quantique SA. http://www.idquantique.com/

7 MagiQ Technologies, Inc. http://www.magiqtech.com/Home.html.

8 QuintessenceLabs Pty Ltd. http://www.quintessencelabs.com/

9 C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. Current status of thDARPA Quantum Network (Invited Paper). In Quantum Information and Computation III, Proc. SPIE, vol.5815, pp.138{149, Orlando, Florida, March 2005.

10 M. Peev, C. Pacher, R. Alleaume, C. Barreiro, W. Boxleitner, J. Bouda, R.Tualle-Brouri, E. Diamanti, M. Dianati, T. Debuisschert, J. F. Dynes, S.Fasel, S. Fossier, M. Fuerst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentchel, H. Hübel, G. Humer, T. Länger, M.Legre, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, E. Querasser, G. Ribordy, A. Poppe, L. Salvail, S. Robyr, M. Suda, A. W. Sharpe, A. J. Shields, D. Stucki, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys. 11(7), 075001/1–37 (2009).

11 Quantum Key Distribution - Industry Specification Group (QKD-ISG), European Telecommunications Standards Institute. http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution.

12 M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express, 19(11), pp.10387–10409 2011.

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

14 M. Fujiwara, T. Domeki, S. Moriai, and M. Sasaki, "Highly secure network switches with quantum key distribution systems," Int. J. Network security 17, pp.34–39 2015.

15 Japanese Patent No. 5791112, "Communication method and communication system," M. Fujiwara and M. Sasaki, Aug. 14th 2015.

16 M. Sasaki. QKD Platform and its Applications. Presentation in Part II Fiber Network, The Fourth International Conference on Updating Quantum Cryptography and Communications (UQCC 2015), Tokyo, Sept. 28, 2015. Recorded video is available in http://2015.uqcc.org/program/index.html

17 NICT press release "Secure communication technology for control and communication of drones," Sept. 28th 2015. http://www.nict.go.jp/press/2015/09/28-1.html

18 M. Sasaki. Tokyo Free Space Optical Testbed. Presentation in Part III Space Network, The Fourth International Conference on Updating Quantum Cryptography and Communications (UQCC 2015), Tokyo, Sept. 28, 2015. Recorded video is available in http://2015.uqcc.org/program/index.html

19 NEC press release Sept. 28th 2015 "Field operation test of the Quantum key distribution system in Cybersecurity factory of NEC for practical application. http://jpn.nec.com/press/201509/20150928 03.html.

20 Toshiba press release June 18th 2015 "Demonstration of Quantum cryptography system."

21 Q. Zhang. Quantum Network in China. Presentation in Part V Relay Talk and Discussion, The Fourth International Conference on Updating Quantum Cryptography and Communications(UQCC 2015), Tokyo, Sept. 28, 2015. Recorded video and slide are available in http://2015. uqcc.org/program/index.html

22 N. Walenta, D. Caselunghe, S. Chuard, M. Domergue, M. Hagerman, R. Hart, D. Hayford, R. Houlmann, M. Legre, T. McCandlish, L. Monat, A. Morrow,

G. Ribordy, D. Stucki, M. Tourville, P. Trinkler, and R. Wolterman. Towards a North American QKD Backbone with Certifiable Security. Contributed talk in the afternoon session on Sept. 28, The Fifth International Conference on Quantum Cryptography (QCrypt2015), Tokyo, Sept. 28{-Oct. 2, 2015, http://2015.qcrypt.net/scientfic-program/

23 W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states," Phys. Rev. Lett. 84(29), pp.4737–4740 2000.

24 H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. 94(23), 230504 2005.

25 X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A72(1), 012326 2005.

26 L. Carter and M. Wegman. New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci, 22:265–279 1981.

27 M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, W. Ogata, and M. Sasaki, "Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing," Sci. Reports, 6, 28988-1-8 2016.

Mikio FUJIWARA, Ph.D

Research Manager, Qunatum ICT Advanced Development Center, Advanced ICT Reseach Institute
Quantum key distribution, Photon detection techology, Cryogenic electronics

Masahide SASAKI, Ph.D

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