Chapter 1

New Quantum Cipher Optical Communication: Y-00

K. Harasawa

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/51107

1. Introduction

1.1. Introduction of Y-00 (overview of network security)

Data volume handled by individuals and companies on the internet is significantly increasing at present. The dissemination of cloud computing causes a lot of important information to flow on networks. And such information is stored in data centers and servers. Meanwhile, cyber terrorism and other crimes that aim at such important information are also on the increase and their techniques have been advanced. To respond to these threats, advanced security measures are implemented in Layer 2 (data link layer) and higher layers of the Open System Interconnection (OSI) reference model. However, safety measures of Layer 1 (physical layer) that forms a transmission path have not been established although Layer 1 is an open area. In such a network broadly two issues exist.

a. For the security of Layer 2 and higher layers cryptography pursuing mathematical complexity is used for decryption calculation. And the basis of safety greatly depends on the performance of computer used by a eavesdropper for decryption. (The safety deteriorates with the increase in performance of computer.)
b. Security hole shifts to Layer 1 and Layer 1 becomes relatively vulnerable when the safety of Layer 2 and higher layers is strengthened.

For this reason, physical security measures are required in Layer 1 to improve safety. Especially in communication lines requiring high safety, measures for constant monitoring through a dedicated optical fiber path of special line route are presented. But such measures require very high running costs and therefore can be realized only for special purposes. Researches on quantum cryptography for the safety of transmission paths have been made all over the world by above-mentioned background [1]. The quantum cryptography currently studied mainly in Japan and Europe is normally the Quantum Key Distribution

(QKD) system using photon transmission. The mainstream of this system is generally called BB84 that was proposed by C.H.Bennett and G.Brassard in 1984 [2]. On the other hand, Y-00 is a new quantum cipher system published by H.P.Yuen(Professor of Northwestern University in US) in 2000 [3]. BB84 uses photon transmission for the QKD system. But Y-00 is the stream cipher system that uses quantum noise existing in continuous light of a laser diode (LD) to directly encrypt data. Y-00, H.P.Yuen and O.Hirota(Professor of Tamagawa University in Japan) made theoretical verification for safety in reports exceeding the Shannon Limit for cryptography in their respective papers for the final version [4]. However, implementation conditions are limited when practical use and dissemination are considered with the current optical communication technology. As one of the Y-00 features, it has been proved that Y-00 is stronger than the current cipher though the ultimate safety (unconditional safety) cannot be achieved by the current technology [5]. Data cannot be completely deciphered by a ciphertext only attack in the currently installed equipment [6]. Also safety can be ensured by the amount of time up to decryption on the fast correlation attack. Y-00 is a physical cipher system and the safety does not depend on calculation amount like general mathematical cryptography. It information hidden by physical phenomena (quantum effect) must be extracted. No shortcut exists because physical working time for extracting this information becomes the basis of safety. Furthermore, the amount of time can be ensured. Astronomical time of this amount of time can be realized also for the currently installed equipment.

1.2. Concept of Y-00

The QKD system that controls photon and transmits data with key information put on a single photon can theoretically show the safety effect provided that One-Time-Pad can be achieved as described in section 1.1. (The absolute condition required by One Time Pad is key distribution that achieves unconditional safety.) To achieve this unconditional safety by single-photon transmission, ideal devices and transmission path are necessary. And various conditions for implementation are really added. These conditions become a loop hole. Therefore that disables absolutely secure key distribution and deteriorates safety level to allow eavesdropping [7,8]. For this reason, the practical use of the QKD system is difficult while maintaining safety in the current optical communication system. Adaptability to large-capacity optical communication networks handling a great deal of information and construction of a new special transmission system at the time of introduction of a security system require much costs.Therefore, applications that are available be limited. Realizing a system by reducing these limiting conditions as much as possible is also an important task. Research and development for Y-00 have been placing the highest priority on the application to existing optical communication systems and possibility that made based on current optical communication technologies. As a result, the WDM transmission system can be shared and no further special infrastructure needs to be constructed. Because Y-00 effectively uses the existing optical modulation system, it can follow up technology trends of normal optical transceiver modules. And it also enables high-speeding, integration, and power saving of the equipment.

2. Principle and outline of Y-00

2.1. Y-00 started from two directions (phase modulation and intensity modulation)

As described above, research of Y-00 was started by H.P.Yuen and other people at the Northwestern University in the United States. Also research and development on implementation are being made at NuCrypt Limited Liability Company (member company of Northwestern University) [9-11]. In this research, phase modulation on coherent light is used as base and encryption is performed by using phase fluctuation (quantum fluctuation) of light. The phase modulation angle of the light becomes multiple value densely. And logic "1" and logic "0" (binary) are distinguished in the 180 degree opposite phase combination. Only one combination is selected from multiple binary combinations (called bases) for each bit from the key information in synchronization with the receiver. The multi-value phase information on the same circumference is closely arranged like overlapping by quantum fluctuation. Eavesdroppers who have no key information must accurately detect phase information. Normal receivers can predict a set of selected base values by using the common key information and therefore can distinguish information. Several-thousands of phase angle values to be used for modulation are set and Non-Linear Feedback Shift Register (NLFSR) and Advanced Encryption Standard (AES) are used for sorting the base to enhance the safety. They use phase modulation for the Y-00 base to apply it to optical space transmission and achieve highly secure communication between aircraft and the ground. In Japan, O.Hirota of Tamagawa University (in Japan) who had made research together with H.P.Yuen started research of Y-00 on the basis of the widely spread intensity modulation of light [12]. Implementation is made by Hitachi Information & Communication Engineering , Ltd. and its application to existing optical fiber networks is considered [13-18].

2.2. Safety of Y-00

Figure1 shows the idea of theoretical safety of Y-00. Theoretical research on ultimate safety of Y-00 is in progress. But if implementation and practicality are considered by present technologies, safety is restricted. However, this restriction can ensure nearly ultimate safety though it is limited by providing essential conditions (astronomical amount of time) for decryption by eavesdroppers through a quantum physical phenomenon. The quantum physical phenomenon means quantum noise (quantum fluctuation) which is an absolute phenomenon that cannot be removed theoretically. Because this phenomenon is completely random, it does not correlate with measured data and the phenomenon cannot be copied. If this phenomenon can diffuse the effect over the signal area, completely decipher is impossible. But differentiation in receiving conditions between normal receiver and eavesdropper is difficult. This will generate trade-off between receiving sensitivity of normal receivers and safety. Therefore ultimate safety cannot be pursued with technical conditions aimed at practical use. Eavesdroppers still cannot avoid physical phenomena of these conditions and acquire correct data. Therefore, direct decryption (cipher text only attack) is impossible. Furthermore, eavesdroppers will attempt to seek for data correlation

to get the initial key from acquired sample data like fast correlation attack that makes exhaustive search. In the exhaustive search, phenomena cannot be copied correctly due to effects of physical phenomena. It is disabling parallel processing [19]. Therefore, eavesdropper must be stacked in serial to find correlation of data. In addition, the sample data volume required for decryption is an order of 1E20~1E30 bytes or more by implementing the safety enhancing measures described later. That memory capacity to store the sample data are 1E20~1E30 bytes or more and the sample data acquisition time is several tens of millions to several hundred millions of years (at 10Gbps transmission) even if effects of physical phenomena cannot be diffused over the signal area as described above. This is limited and that is considered to be indecipherable safety. Because it does not depend on computer's performance unlike the present cryptography that pursues mathematical complexity.

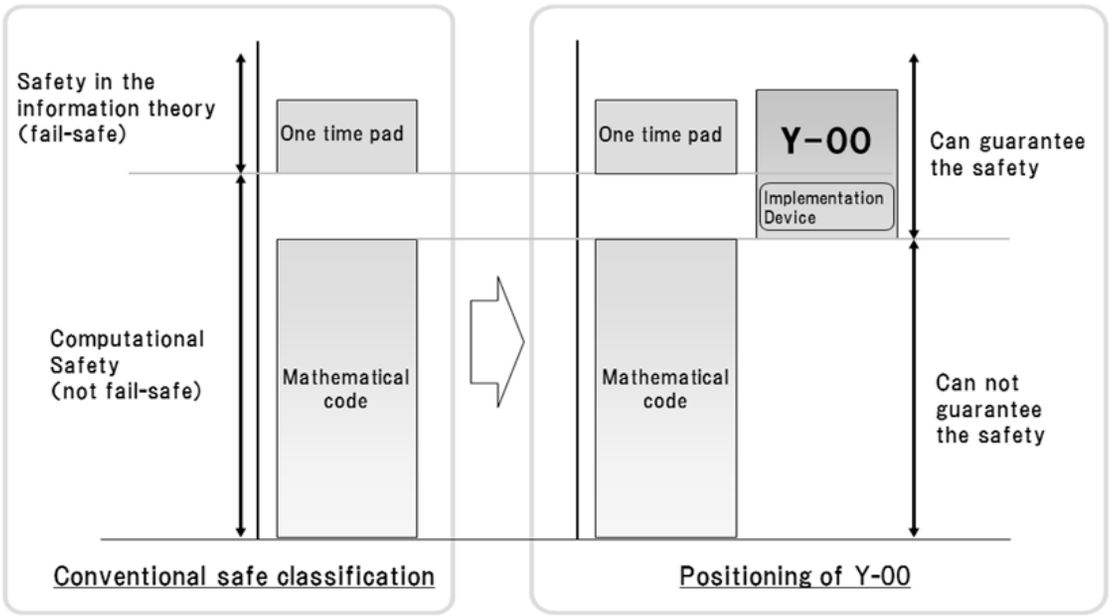

Figure 1. Image of the safety of Y-00

2.3. Idea of physical safety

This section mainly describes an example of optical intensity modulation that is generally used in optical communication. A semiconductor laser diode used in general optical communication uses high-output continuous light (coherent light). The generation probability of each photon that forms this coherent light in the phase and optical power directions is unstable during measurement due to quantum phenomenon, and the value of the probability is not uniquely determined. The distribution of this undefined value is handled as a part of shot noise that is generated during the photoelectric conversion in optical communication, which is an element that degrades the receiving sensitivity. However, effects of other classical noise (including thermal noise of receiving amplifier) generated in the receiver become dominant to the receiving sensitivity of optical

communication using the normal optical intensity modulation system. Normal receivers of the devised optical modulation system in Y-00 can maintain little quantum noise effect as in the case of conventional optical communication system. Also Y-00 produces an effect of significantly degrading the receiving sensitivity (to an unreceivable level) for eavesdroppers. In other words, is established safety by great difference of Signal-to-Noise-ratio (S/N) between at normal receiver and eavesdropper. In this case, safety will be improved by as close as possible to 0.5 the error rate of eavesdroppers. Measured value of quantum noise that affects optical communication varies at completely random against the phase value and power value of light as described in section 2.2. Therefore, the phase modulation system and intensity modulation system used in the existing optical communication can be applied to the Y-00 encryption system that uses this quantum noise. The following describes basic idea to establish safety.

1. Multi-value modulation

The normal optical communication performs a multiple value transfer to increase transmission capacity. However in Y-00, only a single bit out of multiplexed values is used for transmitting information and other values are dummy information for eavesdroppers. It is important for multi-values to establish safety that the quantum noise distribution sufficiently overlaps between adjacent levels (both in optical intensity and phase). The number of values becomes several thousands or more depending on conditions.

2. Encryption and decryption

In the encryption by a transmitter, a combination of binary data (1-bit “1” or “0” level value) is selected for each bit of transmit data from multiple signal values created under conditions (1) using the initial key by the multi-value selection information. This selected binary combination is called base in the same way as phase modulation. The amplitude of this base (between two values) determines the receiving sensitivity of normal receivers in the case of intensity modulation. Therefore, 1/2 (180 degrees for phase modulation) of the maximum signal amplitude is the best value for normal receivers to obtain the optimum receiving sensitivity (Figure2). Decryption process of receiver is essential to distinguish the base that varies in each bit by the best threshold value at signal reception. The amplitude of “1” and “0” levels during reception is estimated based on the multi-value selection information generated by the initial key shared with the transmitter and the threshold value is momentarily moved to the best point to distinguish “1” level and “0” level of the signal. Synchronization of multi-level selection information is critical at this time between the transmitter and receiver. This information is changed at random in each bit between transmitter and receiver (Figure2) [17,18,20-22].

3. Tapping

People other than those who are engaged in optical communication believe in many cases that optical fiber does not be able to tapping unlike electric wires. The principle of optical fiber transmission is well known. Light travels in an optical fiber while repeating reflection using the refraction of light generated by junction of the core and clad in the optical fiber.

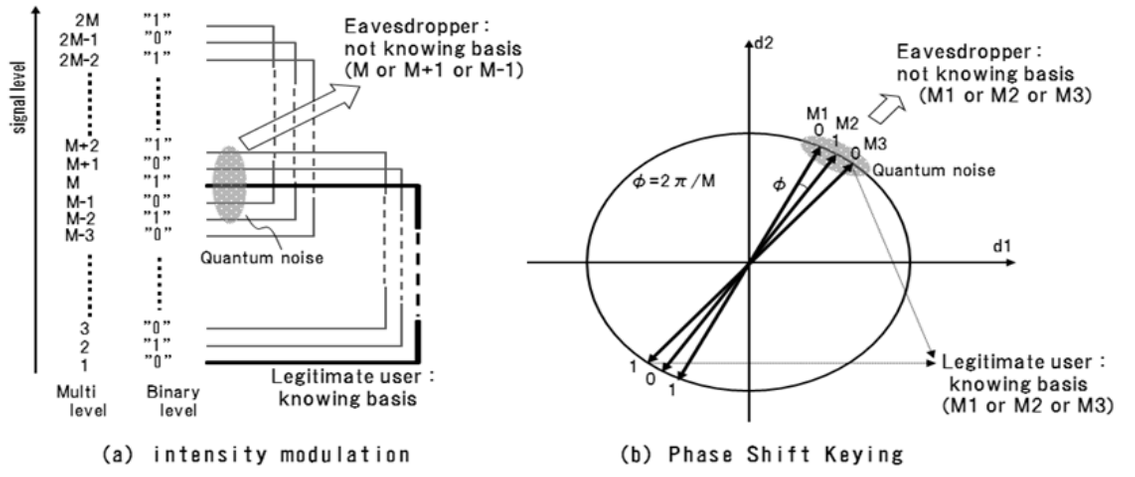

Figure 2. Signal basis and quantum noise

This reflectance varies by bending the optical fiber. If the optical fiber is bent at a sharp angle in particular, the refractive index of the core and clad extremely changes. Therefore optical signal not be able to total reflection. Part of the optical signal will leak out for that. Signal monitoring equipment that uses this principle has been commercialized and used as a measuring instrument. Tapping data from optical fibers has become relatively easy at present due to the technical advance (including high-speed, high-sensitivity detector and low-noise optical amplifier) in optical communication as shown in this example. Measures for improving safety to independently protect transmission paths have become imperative for background mentioned above (Figure3) [22,23].

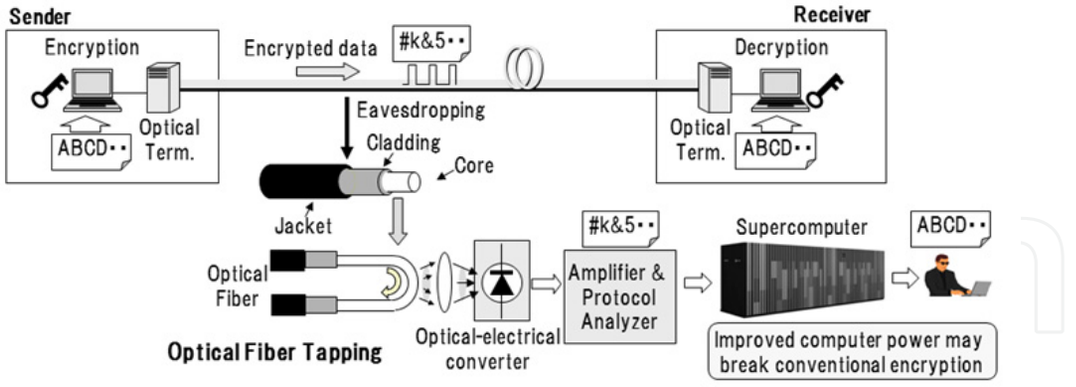

Figure 3. Eavesdropping from optical fiber

3. Implementation of Y-00

3.1. Basic configuration

The Y-00 encryption transmission equipment shares the initial key (Seed Key) between transmitter and normal receiver and performs synchronization processing on each side.

And it configures a pair of transceivers between transmitter and receiver. Figure4 shows the basic configuration of the transmitter of the transceiver. A running key that actually makes encryption is generated from the Seed Key shared by the transmitter and receiver. And the base information (a pair of combination) is selected by the running key from multiple values. Furthermore, the signal level to be used actually is determined from this base information. Input data is converted to a multi-value level by the code modulator and is then output from the subsequent electrical/optical (E/O) converter as a Y-00 encryption optical signal. Figure5 shows the basic configuration of the receiver of the transceiver. The Y-00 encryption optical signal sent from the transmitter is converted to an electrical signal (voltage value) by the O/E converter. And base information is created by the Seed Key in the same procedure as the transmitter. A threshold value that allows the best reception signal to be distinguished is selected from this base information. And a value of 0 or 1 is distinguished by the decoder concurrently with the decoding processing to restore the previous data. This synchronized work between transmitter and receiver performs all processing in each bit of the data transmission rate.

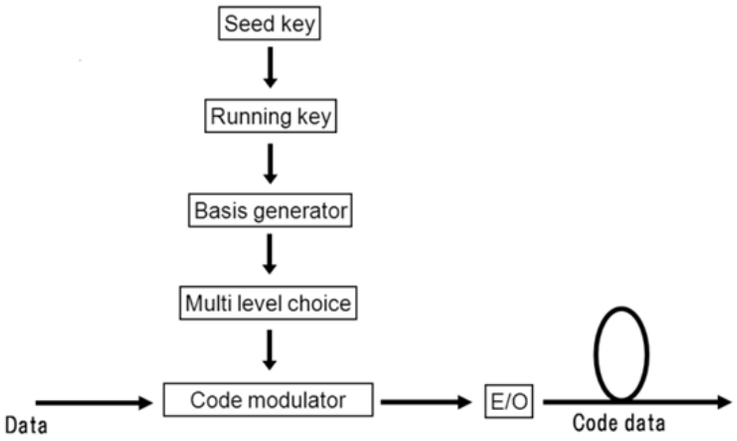

Figure 4. Structure of transmitter of Y-00

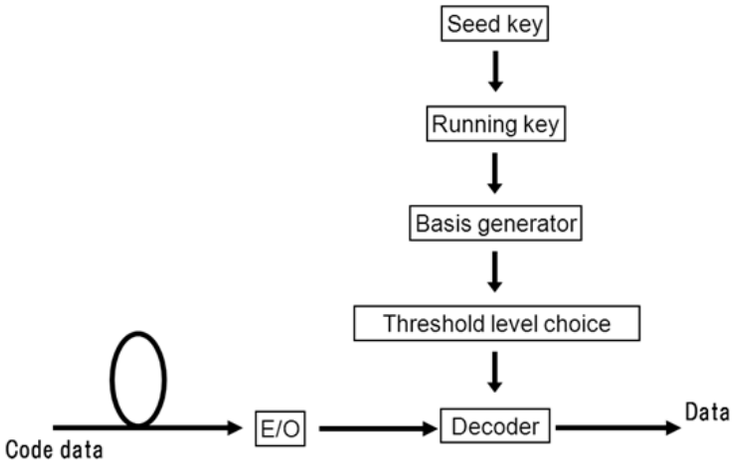

Figure 5. Structure of receiver of Y-00

3.2. Enhancing safety

The probability of eavesdropper's signal level detection error increases with the increase in noise distribution range as described about the safety of Y-00 in the previous section. This effect makes it difficult to extract the correlation of signal level samples acquired by a eavesdropper. Therefore more samples are required. This determines irreducible absolute amount of time necessary to obtain the number of samples required for decryption. This time is for the safety of the people it is possible to secure almost forever (finite strictly) if it is an astronomical value (hundreds of millions of years). Quantum noise contained in coherent light is Poisson distribution dependent on the average optical power as is well known. But this quantum noise is effective between adjacent multi-value levels but it cannot affect entire signal area. For this reason, Y-00 enhances safety using various methods [5,17,18]. This quantum noise effect diffusion method is called Randomization. The following introduces several typical methods.

1. Overlap Selection Keying (OSK)

OSK is a method that allocates logic information (1 or 0) to "High" or "Low" level of light at random to make it difficult for eavesdroppers to decipher signal information "1" or "0" even if they can detect the reception level [16]. Logic of the signal is randomly allocated to a "1" and "0" for each 1bit in order to achieve the OSK. This operation makes it difficult to distinguish whether the signal level detected by tapping is positive logic "1" or negative logic "0". This method is the same as general stream cipher, but is different in purpose and effect. In the basic Y-00, adjacent signal levels are replaced with bit information "1" and "0" alternately. But eavesdroppers can predict the code by focusing on "1" or "0" every other level. Therefore, the safety level is equivalent to the case when the number of values (number of bases) is reduced to 1/2. To solve this problem, changing bit information on a bit basis can maintain degree of difficulty of decryption [12,15,17,24].

2. Keyed Deliberate Signal Randomization (KDSR)

Uniforming the conditional probability of multi-value signal detection in Y-00 is important in terms of cryptographic theory. KDSR is used to perform the uniforming [14]. It is a correction technology that does not directly enhance safety but spuriously evenly expands the quantum noise distribution that is effective for eavesdroppers in detecting the multi-value signal level. This method produces effects equivalent to the case where S/N deterioration effect (overlap of quantum noise between adjacent multi-value signal levels) of eavesdroppers is diffused to a wide area as described in the previous section. Figure6 illustrates this mechanism.

Y-00 of optical intensity modulation is causing a level detection error by the quantum noise distribution overlaps of the adjacent signal level as described in the previous section. It is preferable to uniform the entire multi-value signal level. But it degrades the receiving sensitivity of normal receivers making communication difficult. KDSR slightly fluctuates the selected signal level by shifting a part of multi-value level selections conditions at random to solve this problem. Figure 6 (a) shows this state. The k's true value M is diffused to a range of M±2 by diffusion using KDSR in this example. Furthermore, the noise effect can be

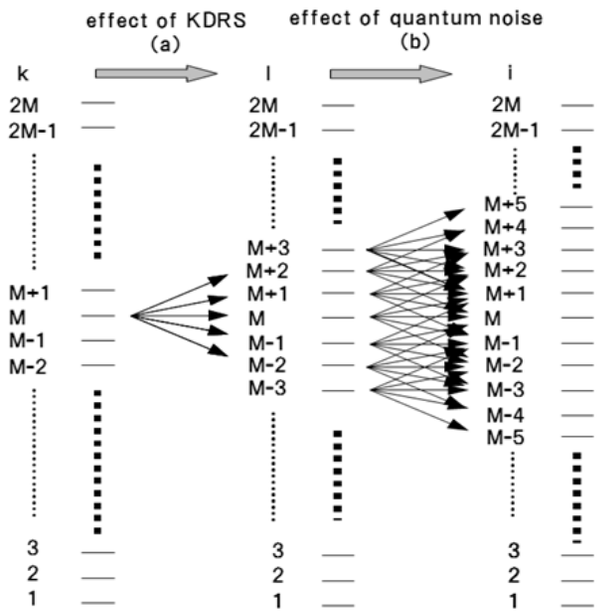

Figure 6. Mechanism of the spread by the random shifter.

diffused to a range of M±5 with the effect of quantum noise distribution (b). The quantum noise distribution function P(k|l) to the individual signal level k diffused by effects of KDSR is evenly arranged, where the l signal level measurement error probability is P(l|i) as the effect of quantum noise at this time. At this time, the effect (a) of KDSR is P(k|l). In addition, the quantum noise effect on the l that are distributed with the effect of (a) is P(l|i). Therefore, the conditional probability P(k|i) of error of true signal level k is shown by the following expression.

$$P(k \mid i) = \sum_{i} P(k \mid l) P(l \mid i) \tag{1}$$

With respect to effects on the receiving sensitivity of normal receivers at that time, the signal level degradation P_{KDS} is shown by the following expression. Conditions are described below. Also ±n is quantum noise diffusion effect by KDSR, 2M is number of multi-values and P_{2M} is full signal amplitude.

$$P_{KDSR} = 2\left(\frac{P_{2M}}{2M}\right)|n| \tag{2}$$

For example, if 2M=4096 and n=±3, the level of effects on normal receivers deteriorates to about 1/683 of the signal's full amplitude power. This effect is slight for normal receivers. The following describes KDSR in terms of quantum noise distribution. Figure7 illustrates the range of effects of signal level "i" on the adjacent level when KDSR is not applied. The quantum noise effect is exerted to the reference level ±2 in this example. For this reason, the base selection information error probability is biased and therefore eavesdroppers can estimate a part of the base selection information more easily. KDSR is applied to the base

selection information that determines base selection as shown in Figure6 to diffuse noise effects on multi-value levels as shown in Figure8 to solve this problem. Thus the bias in the probability distribution of base selection information error is reduced. And making it very difficult to estimate the base selection information [17,25].

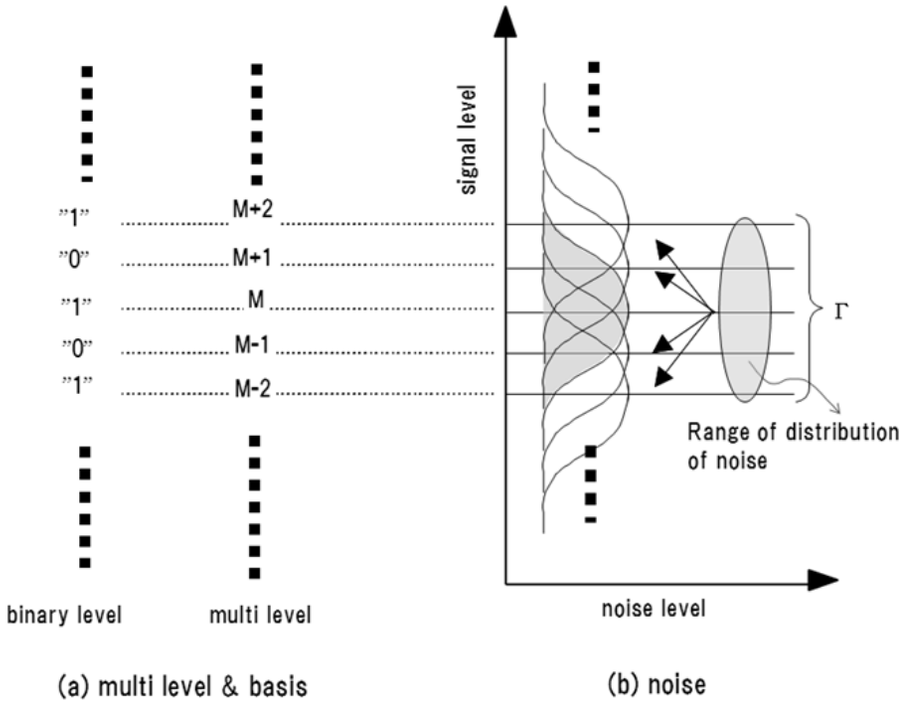

Figure 7. The spread of the noise (KDSR nothing)

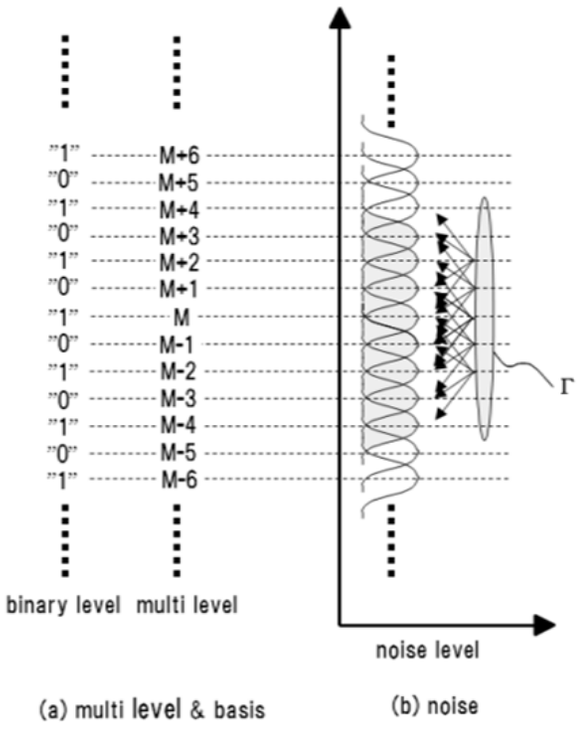

Figure 8. The spread of the noise (KDR)

3. Irregular mapping

Bit error positions become uneven due to effects of the quantum noise distribution in the basic model. Therefore, fast correlation attack may be enabled if the key length is short in the basic array (alternate arrangement of "1" and "0") of bit information of adjacent multi-value levels determined by the base information [25]. However, bit error positions must be uniform to disable such fast correlation attack. Irregular mapping has been developed in order to provide immunity against fast correlation attack even when the short key length [26]. This method disables eavesdroppers to decrypt Y-00 cipher except for complete Brute Force Attack. Figure9 shows the concept of irregular mapping. Synchronization is established between transmitter and receiver. Then bit information is arranged irregularly in the mapping of the multi-value level corresponding to the base. Bit error positions are evenly diffused because the arrangement of the bit information of adjacent multi-value levels is irregular even if the quantum noise distribution effect range is physically the same. This effect disables the fast correlation attack that uses non-uniformity of bit error rate for decryption when the multi-value signal is returned to bit information [17].

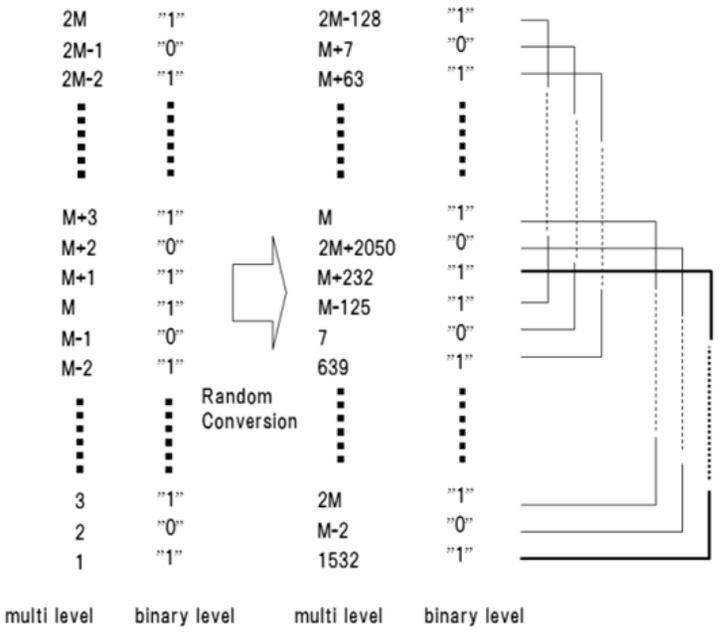

Figure 9. Irregular mapping

3.3. Y-00 encryption circuit

Figure10 shows the configuration of the encryption and modulation circuit that is actually mounted in the Y-00 transmitter. Clock is extracted from input plaintext data for self-synchronization by the Clock Data Recovery (CDR) function. The information for synchronization processing and control is added to the original signal in the Y-00 transmission. Therefore, clock frequency is converted in the FIFO circuit and change the data rate. And frame processing is performed by the framer then information required for

synchronization is added. OSK processing is added to this signal to generate a main signal to be the original signal as described in section 3.1. On the other hand, multi-value level selection signal is generated as follows. Running Key is generated from the Seed Key as a first. Then a base selection signal to be the original signal is generated using the randomly mapped base configuration information. This selection signal generates a multi-level selection signal level after processing by KDSR. The multi-value level selection signal that is the same as the main signal is weighted by each driver circuit and added to determine the multi-value level and generate an encoding signal for encryption of Y-00. The operating principle of this final-stage processing is the same as that of the Digital to Analog (D/A) converter. By driving the optical external modulator using the Y-00 signal generated, the Y-00 encryption signal becomes an optical signal with valid quantum noise effect. [17,18].

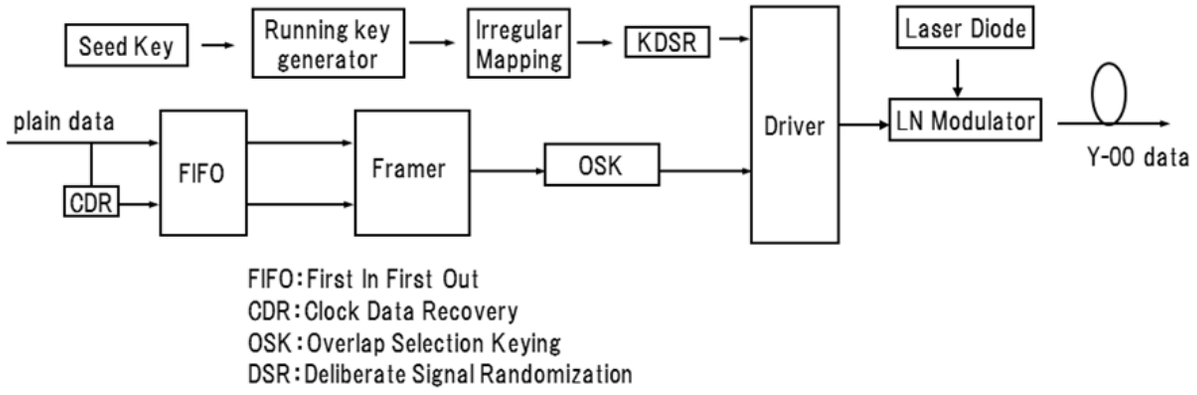

Figure 10. The configuration of the coding of the Y-00 transmitter

3.4. Decoder circuit

Figure11 shows the configuration of the decoder circuit in the Y-00 receiver. The Seed Key information and irregular mapping information are also provided in the receiver as common information. The basic circuit configuration of the decoder is the same as the encryption circuit of the transmitter. However, the receiver does not perform the decoding of KDSR. Therefore, from the decoder outputs a decoding signal (threshold value selection information) of Y-00. The threshold value controller distinguishes the signal on a bit by bit to generate a threshold value level with the best level and timing. Optimum adjustment is made for the threshold level and timing by the Automatic Gain Control (AGC) amplifier and the threshold value controller. Furthermore, the decoder establishes bit synchronization and key synchronization for encryption of Y-00 [17,18].

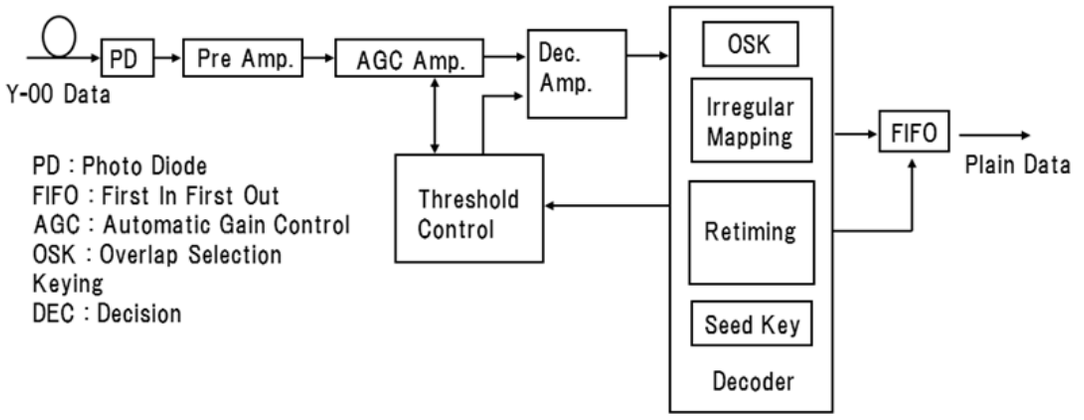

Figure 11. The configuration of the decoding circuit of the Y-00 receiver

4. Transmission experiment and performance evaluation trial production result

4.1. Basic characteristics

To verified the adaptability to existing optical communication networks as Y-00 encryption equipment. Prototype equipment was produced and evaluated based on the content in section 3. The prototype targeted standard specifications of OC-48 (Optical Carrier: SONET standard) optical communication as IEEE standard considering practical use. Table1 shows evaluation results [17]. The transmission rate of original plaintext data is 2.48832 Gbps conforming to OC-48 and the average optical output power is 0 dBm. This is achieved transmission distance of 50 km without relay.

A receiving sensitivity of -15.3 dBm was obtained at a bit error rate (BER) of 1E-12 with a transmission rate of 2.48832 Gbps and an average optical output power of 0 dBm.

Item	unit	result
data rate	Gbps	2.48832
transmission distance	km (w/o amp.)	50
output optical power	dBm (ave.)	0
number of basis (number of levels)	- (-)	2048 (4096)

Table 1. Major characteristics

4.2. Transmission experiment

Low-delay real-time transmission of encrypted uncompressed full-specification High-Definition-Television (HDTV) moving picture data was performed using the prototype Y-00 transmission equipment. Figure12 shows the BER in the back-to-back transmission. The minimum receiving sensitivity is -15.3 dBm when BER=1E-12. The average input power of the

Y-00 transmission equipment (receiver) is approx -10 dBm and the margin of 5.3 dB. It enabling 40 km transmission when considering the optical fiber loss (approx. 0.25 dB/km). Figure13 shows the transmission system in the experiment. The transmitter converts the OC-48 optical signal from 1.5 Gbps moving picture data of signal source by the High Definition Serial Digital Interface to Synchronous Digital Hierarchy (HD-SDI/SDH) converter. And then encrypts the signal by the Y-00 cipher transmission equipment (transmitter). The encrypted optical signal is transmitted through a 40 km single mode fiber (SMF). The receiver decodes encryption signal. And then restores the original moving picture data by the HD-SDI/SDH converter. The latency of the transmission system shown in Figure13 is approx 500 μs. It is achieving secure real-time high-definition moving picture transmission that hardly shows visible delay in monitor images before and after transmission. This result has verified that the Y-00 cipher transmission equipment is applicable to medical sector and financial system networks which require real-time response [27,28].

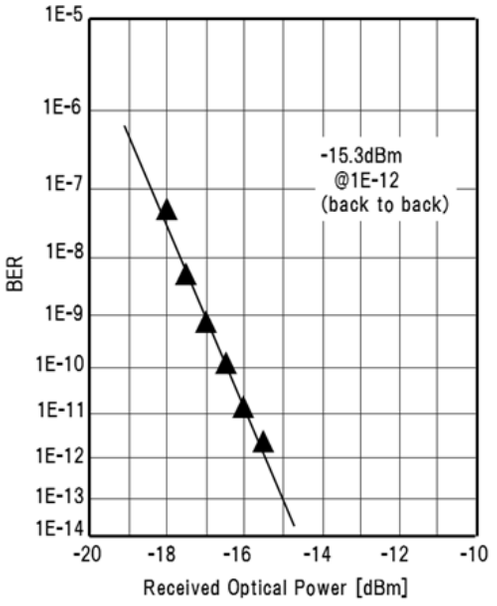

Figure 12. Receiver sensitivity of the regular receiver

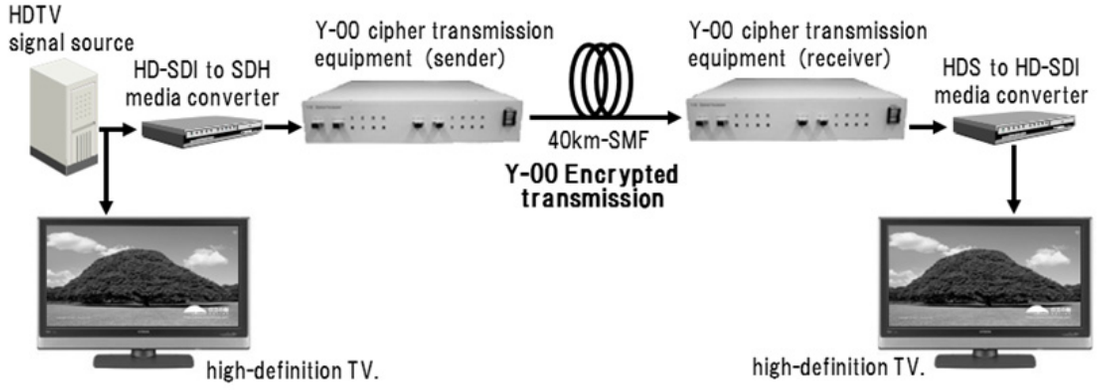

Figure 13. Real-time HDTV transmission experiment

4.3. Field test using a commercial line

We made a transmission experiment using an existing commercial line optical fiber to obtain further prospect of practical use. Figure14 shows the system of the transmission experiment that was actually made. The distance of each transmission span is 48 km and the average span attenuation is 14.5 dB. We made a transmission experiment of total distance 192 km with relay at three location using optical fiber amplifiers (EDFA). Figure15 shows the result of receiving sensitivity measured at the reception end. Figure16 shows waveforms of encrypted and decoded signals. We verified a receiving sensitivity of -18.4 dBm and -19.4 dBm respectively at a BER of 1E-12 in 192 km bidirectional transmission. Also we verified adaptability to optical amplifier repeater transmission. In addition, we have confirmed that the encryption of Y-00 can be applied in Fiber Channel (FC) and Gigabit Ether (GbE). The measured latency value of the transmission system was 1.29 ms in total including the delay of fiber length. Furthermore, we made WDM transmission experiment multiplexing optical output signals from two opposed Y-00 units and verified error-free transmission at each wavelength [17,18,21].

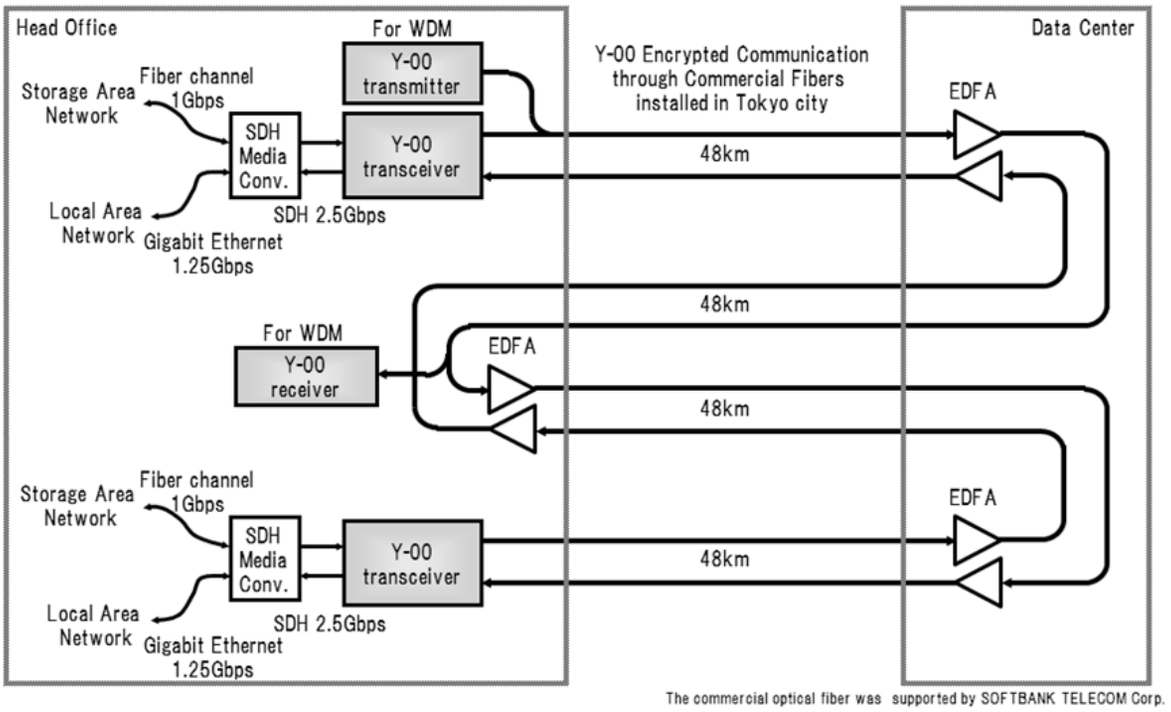

Figure 14. 192 km relay Y-00 encrypted transmission through commercial fibers

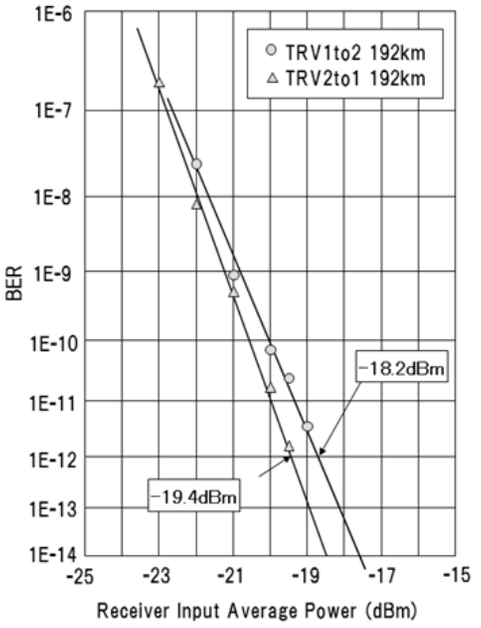

Figure 15. Received optical power sensitivity (192 km)

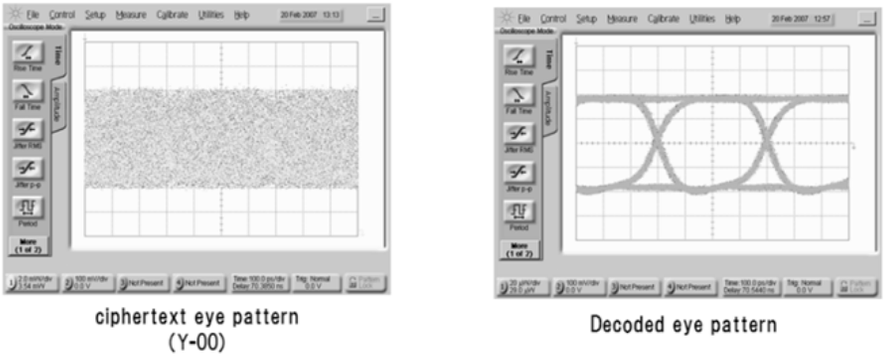

Figure 16. Y-00 transmission wave pattern

4.4. Application to 10 Gbps transmission

This section describes a trial toward large-volume transmission that is the trend of optical communication. Y-00 encryption transmission equipment for 10 Gbps transmission based on optical intensity modulation has been developed in japan [30,31]. The design concept of this equipment is the same as the above-mentioned 2.4 Gbps transmission equipment except that dedicated high-speed devices have been developed to realize the equipment. This section describes the result of 360 km transmission experiment using optical fibers (for experiment laid in Tamagawa University) installed in the field. Figure17 shows the configuration of the transmission system. The 360 km transmission path contains nine EDFA for relay at intervals of 40 km using standard single mode fibers (SMF). Dispersion values are adjusted by the dispersion compensating fiber (DCF) and the tunable dispersion compensator (TDC) to set the residual dispersion to +1170 ps/nm. The optical interface conforms to OC-192. The

optical output power is -1.7 dBm in the back-to-back transmission and the full-amplitude extinction ratio is 2.5 dB. Furthermore, the encryption contains various types of randomization for enhance safety. The transmission path is also provided with an optical preamplifier and an optical bandpass filter in the receiver to ensure the S/N for normal receivers.

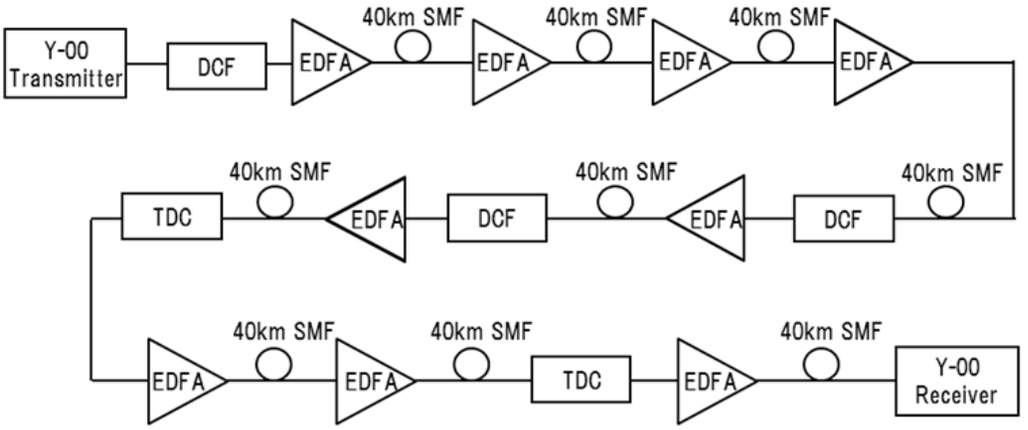

Figure 17. 360 km Y-00 transmission system

Figure18 shows transmission waveforms (eye diagram). They are encrypted waveforms with no eye-opening at each transmission distance. Figure 19 shows characteristic of normal receiver (back-to-back, 40 km, 60 km and 80 km of non repeater transmittion and optical amplifier repeater transmission of 360 km) and the BER of eavesdropper. The minimum receiving sensitivity is -12.2 dBm (BER=1E-12) as shown in Figure 19. And the BER of 360-km transmission is 5.0 × 1E-7. Furthermore, we obtained results that satisfy receiving sensitivity -4 dBm at a BER of 5.0 × 1E-5 which is the target specification considering code error correction under all conditions. We evaluated adjacent signal detection of multi-value signal in the back-to-back transmission to evaluate tapping capability. And obtained a satisfactory result of eavesdropper's BER larger than 0.4. This evaluation has proved that the Y-00 transmission equipment is sufficiently applicable to 10 Gbps transmission. Thus we could obtain prospects for high-speed transmission [29,30,31].

5. Conclusion (future prospects and possibilities)

Based on the Yuen 2000 protocol (Y-00) theory as the research result of H.P.Yuen and O.Hirota, we have developed the Y-00 encryption transmission equipment using quantum noise effects and have verified the practicality of the equipment. We verified the safety and adaptability to existing systems based on trial production results of the equipment and obtained prospects for practical use. The results show the high completeness of the equipment. Hitachi Information & Communication Engineering has been engaged in the development of prototype equipment and is further improving the reliability of the Y-00 encryption transmission equipment for the productization (Figure20). Trial production results show that the Y-00 system can achieve long-haul, large-capacity, high-speed real-

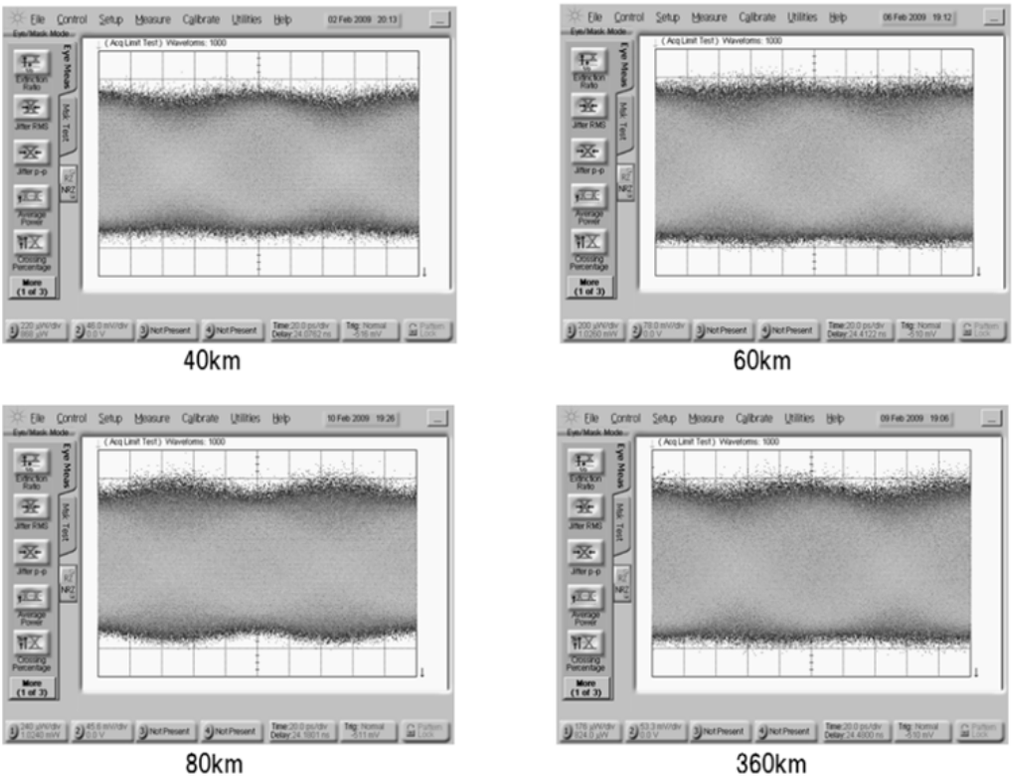

Figure 18. 10 Gbps Y-00 transmission wave form

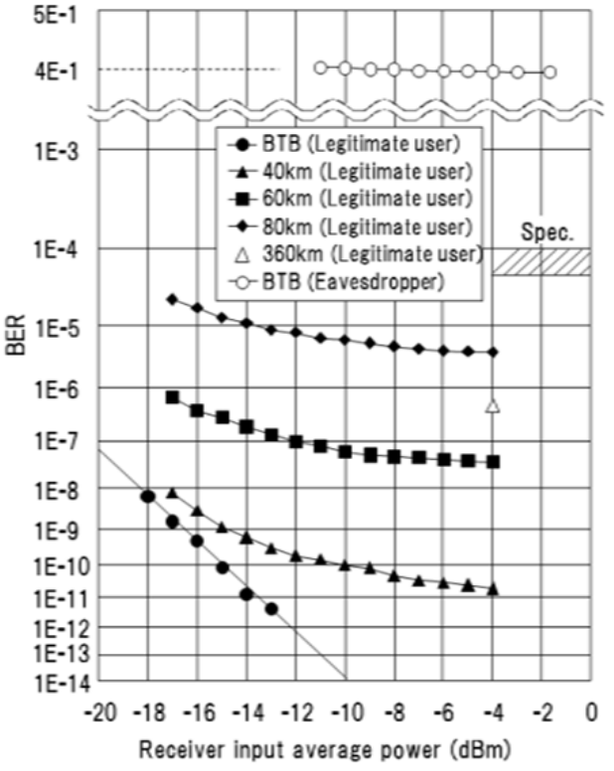

Figure 19. Bit error rate (10 Gbps)

time transmission with low latency. Thus application of the Y-00 system to various fields can be expected. The Y-00 system is also applicable to uncompressed high-definition image transmission in particular, which extends the range of use. Since conventional optical communication technologies that are being developed at present can be used technically, development trends (such as large capacity, downsizing, and power-saving) can be maintained in common. Furthermore, existing optical communication infrastructures are available and allowing co-existence and combined use with current systems and reducing initial costs. Thus we can expect the use of the Y-00 system in wide applications.

Figure 20. Y-00 encryption transmission equipment for the productization

Author details

K. Harasawa
Hitachi Information & Communication Engineering, Ltd., Japan

Acknowledgement

I would like to thank Prof. Osamu Hirota who provided carefully considered feedback and valuable comments. Special thanks also go to Prof. Kiichi Yamashita, Mr.Makoto Honda, Mr. Shigeto Akutus and Mr.Yoshifumi Doi whose opinions and information have helped me very much throughout the production of this study.

6. References

[1] K. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, A. Takada "Security in Photonic Networks: Threats and Security Enhancement", IEEE/OSA Journal of Lightwave Technology, vol. 29, no. 21, p. 3210-3222, 2011.

[2] C. H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, p175-179, December 1984.
[3] H. P. Yuen, “A new quantum cryptography,” Report in Northwestern University, 2000.
[4] O. Hirota, T. Iwakoshi, F. Futami, K. Harasawa, ” Getting around the Shannon limit of cryptography”, SPIE, Newsroom, 10. 1117/2. 1201008. 003069, 2010. http://spie. org/documents/Newsroom/Imported/003069/003069_10. pdf
[5] O. Hirota, “Practical security analysis of a stream cipher by the Yuen 2000 protocol” Physical Review, A 76, 032307, 2007.
[6] K. Kato, O. Hirota, "Randomization techniques for the intensity modulation based quantum stream cipher and progress of experiment", SPIE conference on Quantum Communications and Quantum Imaging Ⅸ, Proceedings vol. 8163, 2011.
[7] I. Gerhardt, Q. Liu, A. L. Linares, J. Skaar, C. Kurtsiefer, V. Makarov, “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”, Nature Communications, vol. 2 349 (14 June 2011)
[8] I. Gerhardt, Q. Liu, A. L. Linares, V. Scarani, J. Skaar, V. Makarov, C. Kurtsiefer, “Experimentally faking the violation of Bells inequalities”, Physical Review Letters, 107, 170404, 2011.
[9] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, H. P. Yuen, “Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks” Physical Review A, vol. 71, 062326, 2005.
[10] G. S. Kanter, E. Corndorf, C. Liang, V. S. Grigoryan, P. Kumar, “Exploiting quantum and classical noises for securing high-speed optical communication networks”, Fluctuation and Noise in Photonics and Quantum Optics III, edited by P. R. Hemmer, J. R. Gea-Banacloche, P. Heszler, Sr., M. S. Zubairy, Proceedings of SPIE, vol. 5842, 2005.
[11] C. Liang, G. S. Kanter, E. Corndorf, P. Kumar, “Quantum Noise Protected Data Encryption in a WDM Network”, IEEE Photonics Technology Letters, vol. 17, No. 7, JULY 2005.
[12] O. Hirota, “Optical Communication Network and Quantum Cryptography”, The Transactions of the IEICE B, No. 4, p478-486, 2004.
[13] K. Harasawa, M. Honda, S. Iwata, N. Kanazawa, T. Kanamaru, O. Hirota, “Basic experiment of quantum cryptography based on optical communications”，Proceedings of the Society Conference of IEICE, Communication, B-10-34, 2004.
[14] T. Hosoi, K. Harasawa, M. Honda, S. Akutsu, Y. Kobayashi, O. Hirota, “Field Transmission Experiment of 2. 5G Y-00 Transmitter/Receiver”，Proceedings of the IEICE General Conference, B-10-80, Communication (2), 419, 2007.
[15] M. Fuse, S. Furusawa, T. Ikushima, O. Hirota, “Development of an ultra high－secure and 1 Gbps optical transmission system using quantum noise diffusion cryptography”, ECOC 2005. 31st European Conference on Optical Communication, Proceedings vol. 3, p555-556, 2005.
[16] M. Shimizu, T. Uno, K. Sako, K. Ohhata, K. Yamashita, K. Harasawa, S. Hirota, “Modulator driver LSI for 10 Gb/s quantum stream cipher optical transceiver using

Yuen-2000 protocol (Y-00)", Proceedings of the Society Conference of IEICE, C-12-8, Electronics (2), 63, 2007・

[17] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, S. Akutsu, T. Hosoi, Y. Doi, K. Ohhata, T. Katayama, T. Shimizu, "Consideration of the Implementation Circuit of Randomization for Physical Cipher by Yuen 2000 protocol", The Transactions of the IEICE C, vol. J91-C, No8, p1-10, 2008.

[18] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, and Y. Doi,, "Quantum encryption communication over a 192 Km, 2. 5 Gbit/sec line with optical tranceivers employing Yuen-2000 protocol based intensity modulation", IEEE/OSA. Journal of Light Wave Technology, vol-29, No. 3, p316-323, 2011.

[19] O. Hirota, K. Kurosawa, "Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol", Quantum Information Processing, vol. 6, No-2, p81-91, 2007.

[20] O. Hirota, T. Shimizu, T. Katayama, K. Harasawa, "10 Gbps quantum stream cipher by Y-00 for super HDTV transmission with provable security", Quantum Communications and Quantum Imaging V, Proceedings of SPIE, vol. 6710, Sep. 25, 2007.

[21] T. Hosoi, K. Harasawa, S. Akutsu, M. Honda, Y. Kobayashi, O. Hirota, "Field Transmission Experiment of 2. 5G Y-00 Transmitter/Receiver", Proceedings of the General Conference of IEICE, Communication (2), 419, B-10-80, 2007・

[22] S Etemad A. Agarwal, T. Banwell, G. Crescenzo, J. Jackel, R. Menendez, P. Toliver, "An Overlay Photonic Layer Security Approach Scalable to 100 Gb/s", Communications Magazine, IEEE, vol. 46, Issue 8, p32-39, 2008.

[23] S. Kay. Miller, "Fiber Optic Networks Vulnerable to Attack", Information Security Magazine, November 15, 2006.

[24] O. Hirota, M. Sohma, M. Fuse, K. Kato, "Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme", Physical Review A -72, 022335, 2005

[25] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, J. Merolla, Security of Y-00 under heterodyne measurement and fast correlation attack, Physics Letters A, 356, p406-410, 2006.

[26] T. Shimizu, O. Hirota, "Randomization of running key for quantum stream cipher Y-00", Technical report of IEICE, OCS, PN, CS, 2007.

[27] Y. Doi, S. Akutsu, T. Hosoi, M. Honda, Harasawa, O. Hirota, T. Katayama, "Hi-Vision Transmission of Y-00 Quantum Cryptography Transceiver", Proceedings of the IEICE General Conference, Communication(2), 328, B-10-45, 328, 2008

[28] Nature Photonics Technology Conference Report, p11, 23-25 October 2007 Tokyo, Japan http://www. natureasia. com/en/events/photonics/2007_photon_conf_report. pdf (accessed 20 April 2012)

[29] S. Akutsu, Y. Doi, T. Hosoi, M. Honda, K. Harasawa, O. Hirota, T. Katayama, "Field Relay Transmission experiment of Y-00 Quantum Cryptography Transceiver", Proceedings of the Society Conference of IEICE, Communication (2), 223, 2007-08-29

[30] Y. Doi, S,Akutsu, M. Honda, K. Harasawa, O. Hirota, S. Kawanishi, O. Kenichi, K. Yamashita, "Field Transmission Experiments of 10 Gbit/s Stream Cipher by Quantum

Noise for Optical Network", Proceedings of the IEICE General Conference, Communication(2) 2010, 369, 2010.

[31] O. Hirota, K. Ohhata, M. Honda, S. Akutsu, Y. Doi, K. Harasawa, and K. Yamashita, "Experiments of 10 Gbit/sec quantum stream cipher applicable to optical Ethernet and optical satellite link", SPIE conference on quantum communication and quantum imaging VII; Proceedings of SPIE, vol. 7465, 2009.

IntechOpen