ISSN 2186-6570

Two Months Field Transmission Test of 2.5-Gb/s Y-00 Cipher in 160-km (40 km x 4 spans) Installed Optical Fiber Cable for Secure Optical Fiber Communications

Fumio Futami and Osamu Hirota

Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.2, No.1, 15-17, 2012

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.2 No.1 : 15-17 (2012)

Two Months Field Transmission Test of 2.5-Gb/s Y-00 Cipher in 160-km (40 km × 4 spans) Installed Optical Fiber Cable for Secure Optical Fiber Communications

Fumio Futami and Osamu Hirota
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa Gakuen, Machida, Tokyo, 194-8610, Japan
E-mail: futami@lab.tamagawa.ac.jp

***Abstract*— Field transmission test of 2.5-Gb/s Y-00 cipher in 160-km (40 km × 4 spans) is demonstrated in the installed optical fiber, TAMA net #1, for secure optical fiber communications. A long term investigation of an intensity modulated Y-00 transmitter and receiver with signal intensity levels of 4096 is conducted and the bit error rate of < 10^{-9} for two months is successfully achieved.**

***Index Terms*— noise masking, physical cipher, secure communication, Y-00 protocol**

I. Introduction

Security in optical data link of local area networks and wide area networks is an issue especially for data centers providing services of the cloud computing where confidential information is transmitted. The use of the physical cryptography whose security relies on the physical effect is a promising way for enhancing the security of optical data link together with the mathematical encryption. The quantum stream cipher by Yuen 2000 protocol (Y-00) is noise-based physical layer encryption and has a possibility that realizes the unbreakable security level [1]. It also features high compatibility with the current optical fiber communication systems and is suitable for high-speed (> Gb/s) communication. It employs dense M-ary keying (multi-level modulation) for the binary information to realize security, which requires no excess bandwidth. A fundamental idea of Y-00 cipher to avoid eavesdropping is shown in Fig. 1. The noise masks the Y-00 cipher signal level and disables the correct level discrimination of an eavesdropper. Prototypes of Y-00 cipher transceiver using multi-level phase modulation (PSK Y-00) [2] and intensity modulation (ISK Y-00) [3] have already been developed. We have focused on the research of ISK Y-00 since it has an advantage of simple configuration. So far, we demonstrated ISK Y-00 at 2.5 Gb/s using signals with the intensity level number of upto 4096 [4,5], and at 10 Gb/s and 40 Gb/s using 64-intensity level signals [6,7]. In the reports, transmission performances were usually investigated in optical fibers in the laboratory, and investigation terms were several hours at longest. However, for practical use, a longer term investigation is desirable in optical fibers installed in the field.

In this work, we demonstrate a long term investigation of an ISK Y-00 transmitter and receiver in the field optical fiber transmission line, TAMA net #1. The transmitter has signal intensity levels of 4096 and bit rate of 2.5 Gb/s. The Y-00 signal is transmitted over 160 km of the optical fiber installed in the field. The transmission line consists of 4 spans of a 40-km standard single mode optical fiber (SMF) and an optical amplifier. Error free operation of the bit error rate (BER) < 10^{-9} for two months is successfully demonstrated.

II. Y-00 Quantum Cipher

The process of an eavesdropper to steal the secret key or the information from the chipertext generally consists of two steps. The first step is to read the ciphertext correctly. The second step is that the ciphertext is processed mathematically to recover the secret key or the plaintext, that is, the original information before encryption. Y-00 quantum cipher makes the first step difficult by using multi-level encryption of "basis that sends the binary data".

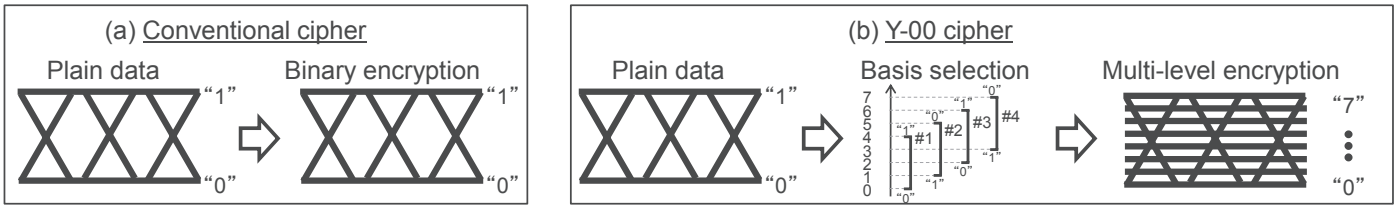

Fig 1. Comparison of (a) conventional cipher and (b) Y-00 cipher (number of basis, M = 4).

Figure 1 compares the conventional cipher and the Y-00 quantum cipher. In general, the conventional cipher based on the mathematical encryption converts binary data of plaintext into binary data of ciphertext. Since an eavesdropper can discriminate the two correct signal levels, "0" and "1", of the ciphertext, he can succeed in acquiring the ciphertext. On the other hand, in the case of Y-00 quantum cipher, the binary data is encrypted thorough the multi-level encryption by using the set of basis. When dense multi-level signals are employed for Y-00 signals and the noise amount is designed to be larger than the minimum decodable signal difference of the multi-level signals, the noise masks the signal level and hence the correct signal level detection, that is, the ciphertext reading, can be avoided. As a result, the security level of the Y-00 quantum cipher is higher than that of the mathematical encryption for an eavesdropper. It should be noted the legitimate user with the secret key knows the basis of each signal and he can process the observed encryption signal to recover the original information.

III. Y-00 Quantum Cipher Transmitter and Receiver

Figure 2 shows basic functions of a transmitter and a receiver of Y-00 quantum cipher. In the transmitter, a running key is generated in a linear feedback shift register (LFSR) circuit by extending a seed key which is shared in the transmitter and receiver. In an overlapped selection keying (OSK), the polarity of the input binary data is scrambled based on XOR operation between input binary data and the running key. On the other hand, basis conveying bit signals are generated in the following steps. First, a block of bits from the LFSR output with the bits' length of $\log_2 M$ (M: number of basis) is produced in the M-ary circuit. The sequence of the block is a running key. Next the running key is scrambled by a mapper. The information bit is modulated by Y-00 driver with the scrambled running key in a bit-by-bit manner to generate multi-levels, 2M, of electrical signals. The multi-level electrical signals modulate an external modulator to generate Y-00 signals with the multi-levels of 2M.

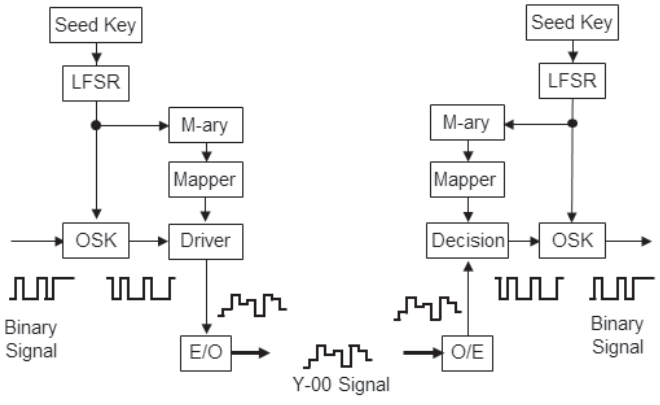

Fig.2. Schematic of the transmitter and receiver.

IV. Field Transmission Test

A long term transmission experiment was demonstrated by using the above-mentioned transmitter and receiver. As a transmission line, TAMA net #1 was employed. The optical fibers are installed under the ground in Tamagawa University. The length of each optical fiber span is 40 km. Every 40 km, an EDFA amplified the signals. The net length is 160 km. The input power into each span was set to – 3 dBm. The transmitter and receiver and optical repeaters are placed in our laboratory.

In the transmitter end, the 2.5-Gb/s Y-00 signal with a wavelength of 1547.6 nm and with the number of intensity levels of 4096 ($M = 2^{11}$) was generated. In the receiver, Y-00 signal was detected by a PIN photodiode (PD) followed by a transimpedance amplifier (TIA). The received RF signal was divided for clock recovery (CR) and data recovery. For data recovery, the decision threshold was adjusted in a bit-by-bit manner depending on the threshold information defined from the shared key. The received data was deciphered and input to a bit error rate (BER) tester to measure BERs of the deciphered signals. An optical preamplifier was employed and the PD input power was adjusted by an optical attenuator in the receiver. It should be noted that the signal-to-noise ratios (SNRs) for the legitimate user and an eavesdropper were different. The shared key has information on the threshold. Therefore, the SNR for the legitimate user is much higher than that for the eavesdropper.

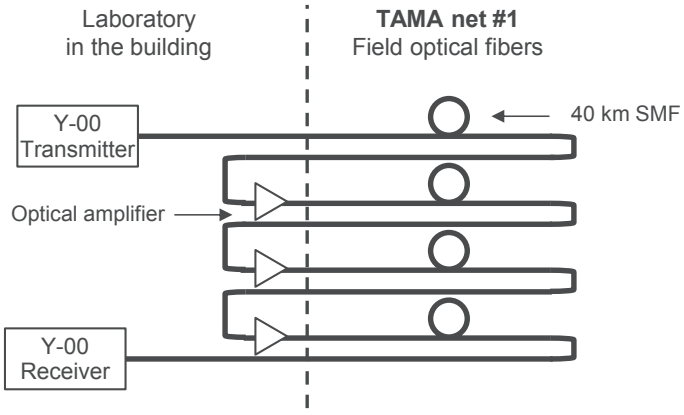

Fig.3. Schematic of the 160-km transmission experiment in the TAMA net #1, an installed optical fiber.

Waveforms were observed by a sampling oscilloscope after 160-km transmission. Y-00 signals were converted to the electrical signal by the direct-detection with a PIN photo-diode followed by a transimpedance amplifier and a limiter amplifier. Waveforms of the Y-00 signal and deciphered binary signal measured with the persistence time of 12 hours are shown in Figs. 4. The Y-00 signal waveform (Fig.4 (a)) looked rather noisy since it had 4096 intensity levels. However, clear eye opening was observed after deciphered to the binary signals (Fig.4 (b)). The error free transmission over 160 km was confirmed for 12 hours. Next, bit error rates (BERs) were measured in every 10 minute for two months. The outside air temperature ranged from ~20 °C to ~35°C during the BER

measurements. As shown in Fig.5, BERs were maintained to be less than 10^{-9} during the whole measurement duration. Some variations of the BER were observed, which stemmed from the changes of the transmission fiber condition due to the outside air temperature change, vibration by cars and so on.

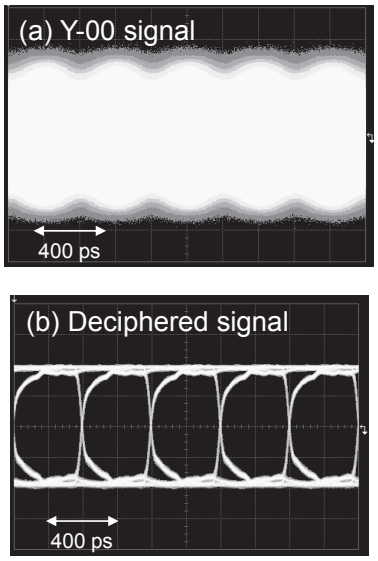

Fig.4. Waveforms of Y-00 and deciphered signals measured for 12 hours.

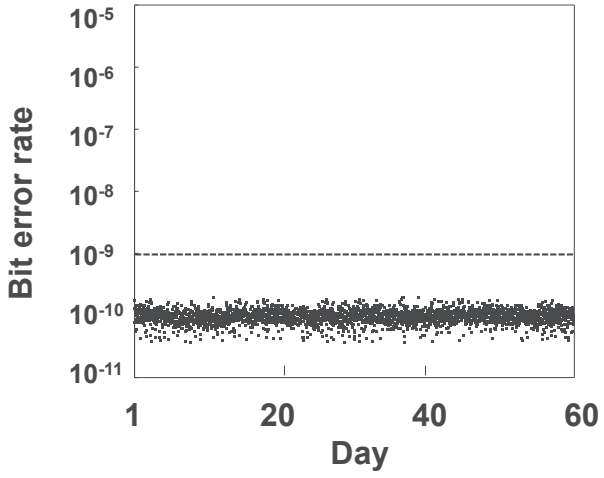

Fig.5. BER characteristic experimentally measured for two months.

V. Conclusion

In conclusion, it has been demonstrated that the long term investigation of an ISK Y-00 transmitter and receiver in the optical transmission line, TAMA net #1, installed under the ground in Tamagawa University. The number of signal intensity levels was 4096, the bit rate was 2.5 Gb/s and the transmission distance was 160-km. Although small variations of BERs were measured due to the condition change of the transmission optical fiber due to the temperature change, vibration, and so forth, the error free operation of BER < 10^{-9} was achieved for two month. According to the long term BER measurement result, the authors believe that the transmitter and receiver is now ready for practical use. As the next step, we focus on the downsizing of the transmitter and receiver, longer distance transmission, and higher capacity communications. The detail security performance is also a natural extension of the work.

Acknowledgment

This work was supported in part by Fujitsu Laboratories Ltd.

References

[1] O. Hirota, “Practical security analysis of quantum stream cipher by Yuen 2000 protocol,” Phys Rev A, 032307, 2007.

[2] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure communication using mesoscopic coherent states,” Phys. Rev. Lett., vol.22, 227901, 2003.

[3] O. Hirota, M. Sohma, M. Fuse, and K. Kato, “Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme,” Phys. Rev. A, 72, 022335, 2005.

[4] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, T. Hosoi, and Y. Doi, “Quantum encryption communication over a 192-km 2.5-Gbit/s line with optical transceivers employing Yuen-2000 protocol based on intensity modulation,” J. of Lightwave Technol. vol. 29, no. 3 , pp.361-323, 2011.

[5] F. Futami and O. Hirota, “Masking of 4096-level intensity modulation signals by noises for secure communication employing Y-00 cipher protocol,” 37th European Conference on Optical Communication (ECOC), Tu.6.C.4, 2011.

[6] Y. Doi, S. Akutsu, M. Honda, K. Harasawa, O. Hirota, S. Kawanishi, K. Ohhata, and K. Yamashita, “360 km field transmission of 10 Gbit/s stream cipher by quantum noise for optical network,” Optical Fiber Communication Conference (OFC), OWC4, 2010.

[7] F. Futami and O. Hirota, “40 Gbit/s (4 × 10 Gbit/s) Y-00 Protocol for Secure Optical Communication and its Transmission over 120 km,” Optical Fiber Communication Conference (OFC), OTu1H.6, 2012