ISSN 2186-6570

Experimental Observation of Masking Intensity-Modulation Y-00 Signals at 10 Gb/s by Noise for Secure Optical Communication

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.1, No.1, 29-31, 2011

Experimental Observation of Masking Intensity-Modulation Y-00 Signals at 10 Gb/s by Noise for Secure Optical Communication

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— **An experimental measurement of intensity noise masking of Y-00 signals at a bit rate of 10 Gb/s is demonstrated for the first time to our knowledge. 64-level intensity modulation signals for secure optical fiber communications by Y-00 protocol are measured by the direct detection and it is shown intensity noise masks more than 14-signal levels disabling correct signal level discrimination by an eavesdropper's direct detection measurement.**

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

I. Introduction

Secure optical communications in the physical layer has recently attracted considerable interest since personal information and confidential information are transmitted in the network. A method of achieving secure data transmission with high data rates and avoiding information leakage through tapping optical signals from transmission fibers is attractive especially for data centers providing services for the cloud computing. For practical use, it is desired secure communications are compatible with current optical fiber communication. The use of the physical cryptography whose security relies on the physical effect is a promising way for providing the security of optical links together with the mathematical encryption. An optical code division multiplexing (OCDM) technique [1,2] and a cipher based on Y-00 protocol [3,4] are physical cryptographies suitable for high-speed (>Gb/s) optical fiber communication systems. The latter is noise-based physical layer encryption and employs dense M-ary keying (multi-level modulation), which requires no excess bandwidth. From the practical viewpoint, Y-00 has an advantage of the use of components widely utilized in the current optical fiber communication systems. Therefore Y-00 has high compatibility with the existing infrastructure of optical fiber communication systems. Wavelength division multiplexing (WDM) technique is easily applied. It also features that cipher texts are difficult to be read correctly by an eavesdropper. This feature leads to the protection of cipher-breaking and storing in memories by eavesdroppers who have no correct key. Prototypes of Y-00 cipher transceiver using multi-level phase modulation (PSK-Y00) [3] and intensity modulation (ISK-Y00) [4] have already been developed. A distinguished feature of Y-00 cipher is to mask the encrypted signals employing dense M-ary keying for the binary information by the noise to improve security. It has been theoretically discussed the masking effect by the noise [5]. So far, we have demonstrated experimental observation of the masking effect of 2.5-Gb/s Y-00 signals by measuring waveforms with the direct detection [6,7].

A research direction is to expand the capacity to meet the increasing traffic demands. 10-Gb/s Y-00 transmission experiment over 360 km has been already demonstrated [8]. However, noise masking of 10-Gb/s Y-00 signals has not been investigated. In this work, we focus on the experimental observation of the masking effect of 10-Gb/s Y00 signals by means of the direct detection. We demonstrate masking measurement of 10-Gb/s Y-00 signals with 64-level intensity modulation and it is shown the intensity noise masks more than 14 signal intensity levels.

II. Y-00 Cipher Signals

In attacking cipher signal process by an eavesdropper, there are generally two steps. The first step is to read correctly the encrypted data (ciphertext). The second step is the mathematical processing of the ciphertext to recover the original data (the plain text) or the secret key. Y-00 protocol makes the first step difficult by using multi-level encryption of "basis that sends the binary data".

Figure 1 compares conventional cipher and our cipher based on Y-00 protocol. In general, the conventional cipher based on the mathematical algorithm converts binary data of plaintexts into binary ciphertexts. Therefore, an eavesdropper can easily distinguish the two correct signal levels ("0","1") of the ciphertext, resulting in the eavesdropper's success of acquiring the correct ciphertext itself, which might lead to the cipher breaking. On the other hand, a basic concept of Y-00 cipher is to utilize the noise for making it difficult to read the cipher text, i.e., to discriminate the correct signal level by using dense multi-level signal encryption. An eavesdropper is forced to detect the correct intensity levels of the dense multi-level

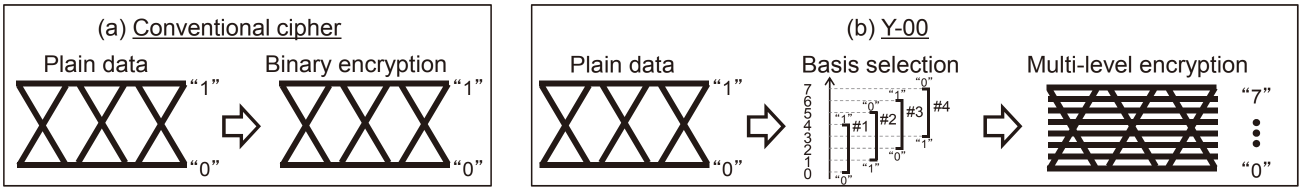


Fig.1. Comparison of signal waveforms before and after encryption. (a) conventional cipher and (b) Y-00.

signals. When the noise amount of Y-00 cipher signals is set to be larger than the minimum difference of Y-00 signal intensity levels, the noise masks Y-00 cipher signal and hence the correct signal level detection can be avoided. It should be noted the legitimate user with the secret key can process the encrypted data to recover the original information.

For evaluation of the masking effect, we define a parameter meaning the number of signal levels masked by the intensity noise as

$$\Gamma = \frac{\sigma}{\Delta} \tag{1}$$

where σ and Δ denote the magnitude of intensity noise, and a difference between two neighboring signal intensity levels, respectively. In the region of $\Gamma > 1$, the intensity noise of a signal level penetrates into neighboring signal levels, which plays as a barrier against the eavesdropping.

III. Y-00 Cipher Transmitter

The schematic of the transmitter [9] is shown in Fig.2. A running key is generated in a linear feedback shift register (LFSR) circuit by extending the key length based on a seed key (a common key) which is shared in the transmitter and receiver. In an overlapped selection keying (OSK) based on XOR operation between input binary data and the running key, the polarity of input binary data is scrambled. On the other hand, basis-level selection signals are generated in the following steps. First, a block signal with bit length of $\log_2 M$ (M: number of basis level) of the LFSR output is produced in the M-ary circuit. M value is adjustable from 1 to 5. Next the block signal is scrambled by a mapper. The scrambled input binary data are modulated by the running keys in a bit-by-bit manner to generate multi-level (2^{M+1}) signals. In an E/O intensity modulator, Y-00 optical signals are generated by intensity modulation of a light with the multi-level electrical signal, where a bias voltage is given to induce optical offset.

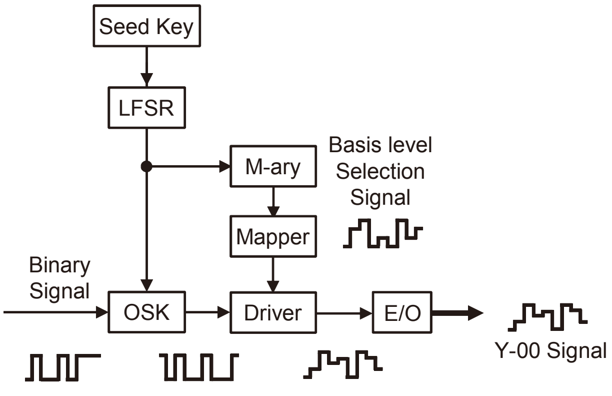


Fig.2. Schematic of the transmitter.

IV. Experiments

Experimental observation of masking Y-00 signals was demonstrated by using a Y-00 cipher transmitter operating at a bit rate of 10 Gb/s at a wavelength of 1553.5 nm. As shown in Fig.3, the 10-Gb/s Y-00 signals from the transmitter were converted to the electrical signal by the direct detection with a PIN photodiode followed by a transimpedance amplifier and a limiter amplifier. Electrical signals were observed by a sampling oscilloscope. The bandwidth of the measurement setup was about 10 GHz. The average input power into the photodiode was set to -10 dBm.

First, the number of the signal intensity levels was set to 4 (M = 1) so that the noise distributions were clearly measured. Figure 4 (a) shows the waveform of Y-00 signals and the intensity noise distribution measured by counting the number of sampling bins around the center of the eye diagrams. Four peaks corresponding to the four signal intensity levels were clearly observed and the amounts of the noise were almost the same of 4.9 mV, although the signal and ASE beast noise was dominant under the current receiver condition. This was due to the saturation characteristics of the limiter amplifier. Measured Δ was 14.5 mV resulting in Γ = 0.3.

Next, the number of the signal intensity levels was increased to 64 (M = 5). The sampling waveform in Fig.4(b) did not show clear eye-opening due to masking effect by the intensity noise. The measured noise distribution in Fig.4(b) was almost uniform. From the noise amount measured for the signal of 4 intensity levels, we can derive Γ for other M values (2 ~ 5) which is plotted in Fig.5. It is shown that in the case the number of signal intensity level was 64, about 14.2 signal levels were masked by noise. It is obvious that the correct levels of the 64 intensity level signals cannot be discriminated by merely observing the signal waveforms with the direct detection.

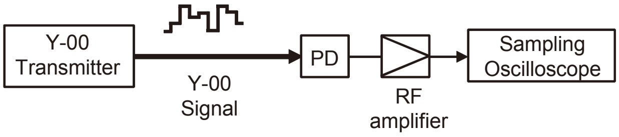
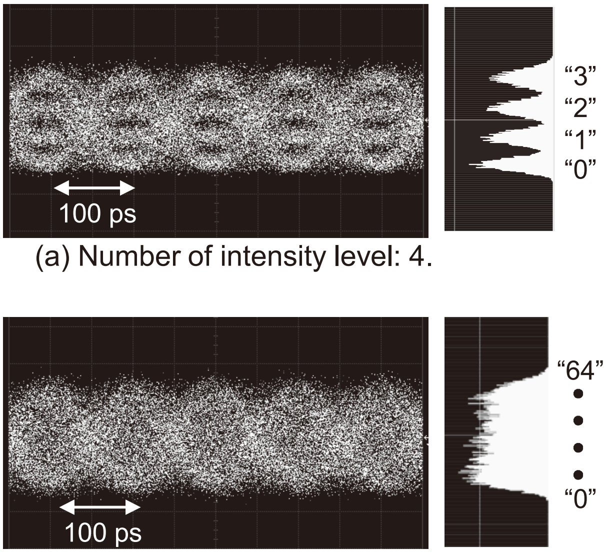


Fig.3. Experimental setup for measuring masking of Y-00 signals.



(a) Number of intensity level: 4.

(b) Number of intensity level: 64

Fig.4. Waveforms (left) and intensity noise distributions (right) of Y-00 signals. Number of signal intensity levels: (a) 4 , (b) 64.

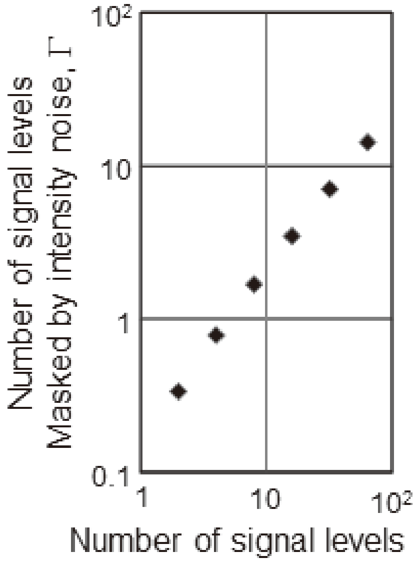


Fig. 5. Number of signal levels masked by intensity noise as a function of number of signal intensity levels.

V. Conclusion

We have measured experimentally noise masking of Y-00 signals at a bit rate of 10 Gb/s by the direct detection. Y-00 signals have 64-level intensity modulation for secure optical communication. Masking the Y-00 signal levels by noise has been successfully observed and it has been shown that 14.2 intensity levels are masked. The result shows that the correct signal level discrimination is not possible by merely observing the waveforms using the direct detection. Y-00 is a promising method for achieving secure data transmission with high data rates. It is expected Y-00 protocol is applied to actual optical fiber transmission systems for secure communications.

Acknowledgment

This work was supported in part by Fujitsu Laboratories Ltd.

References

[1] G. D. Crescenzo, R. Menendez, and S. Etemad, "OCDM-based photonic encryption with provable security," in Proc. Optical Fiber Communication Conference (OFC), OTuP3, 2008.

[2] G. Cincotti, N. Wada, and K. Kitayama, "Secure optical bit- and block-cipher transmission using a single multiport encoder/decoder," in Proc Optical Fiber Communication Conference (OFC), JThA93, 2008.

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

[4] 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.

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

[6] F. Futami and O. Hirota, "Experimental Observation of Masking Y-00 Cipher Signal Levels by Intensity Noise," in Proc. Opto-Electronics and Communications Conference (OECC) , 5A3-2, 2011.

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

[8] 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," in Proc. Optical Fiber Communication Conference (OFC), OWC4, 2010.

[9] 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.