ISSN 2186-6570

Transmission of 100 Gbit/s (10×10 Gbit/s) Y-00 Quantum Stream Cipher for Secure 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.4, No.1, 15-17, 2014

©Tamagawa University Quantum ICT Research Institute 2014
All rights reserved. No part of this publication may be reproduced in any form or by any means electrically, mechanically, by photocopying or otherwise, without prior permission of the copy right owner.

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.4 No.1 : 15-17 (2014)

Transmission of 100 Gbit/s (10 × 10 Gbit/s) Y-00 Quantum Stream Cipher for Secure 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—
For secure and high capacity optical fiber communications, WDM transmission experiment of 100-Gbit/s quantum stream cipher is demonstrated by Y-00 protocol with 64-level intensity modulation. Error-free transmission (bit-error rate < 10^{-9}) in an 120-km amplifier repeated fiber link is successfully achieved.

***Index Terms*— Y-00 protocol, stream cipher, physical cipher, secure optical access system,.**

I. Introduction

Data security in the physical transport layer of optical fiber transmission is an issue, because optical signal tapping from transmission optical fibers is achievable, and eavesdropping information from such tapped optical signals may be possible. The mathematical encryption is sometimes employed and features practical, however, it has a risk that it can be solved once a cipher-breaking algorithm is discovered.

Physical cipher whose security relies on the physical effect is promising to realize more secure cipher than the mathematical encryption itself. By combining the physical cipher and the mathematical encryption, the degree of security of the optical link is naturally enhanced. Therefore, the development of a practical physical cipher is of importance. DARPA started a project developing physical cipher featuring high speed and long transmission distance utilizing macroscopic scheme [1]. Secure physical-layer transmission using space-division multiplexing [2] and physical ciphers such as optical code division multiplexing (OCDM) technique [3,4] and stream ciphers by Yuen-2000 protocol, so called, Y-00 quantum stream cipher [5,6] are suitable for secure, high-speed (>Gb/s) and long distance optical fiber communication.

Y-00 quantum stream cipher or simply Y-00 is noise-based physical layer encryption and is an example of the "Quantum Enigma Cipher" [7] which is a term defined by Tamagawa University as a new concept in the cryptography that may break the Shannon limit of the cryptography using a pseudo-random number generator (PRNG) and physical randomness. It employs dense M-ary keying (multi-level modulation), which requires no excess bandwidth and features the use of components utilized in the current optical fiber communication systems. A fundamental idea to avoid eavesdropping is to mask the signal level of ciphertext by the noise disabling the correct level discrimination by an eavesdropper. Prototypes of a transceiver using multi-level phase modulation (PSK Y-00) [5] and intensity modulation (ISK Y-00) [6] have already been developed. So far, we demonstrated ISK Y-00 at 2.5 Gb/s by using 4096-intensity level signals [8,9] and at 40 Gb/s using 64-intensity level signals [10]. For practical use, a longer term test of the 2.5-Gb/s transceiver over 60 days was successfully demonstrated in optical fibers installed in the field [9]. The transceiver was successfully applied to the experimental test in the in-service GbE network of our University. Quadrature amplitude modulation (QAM) is employed for the physical cipher [11,12].

In this work, we focus on increasing the capacity to meet increasing traffic demands. Y-00 features high compatibility with the existing infrastructure of optical transport layer, and data capacity increasing is easily realized by the wavelength division multiplexing (WDM) technique. Here, the authors report on 100 Gb/s WDM ISK Y-00 transmitter (TX) and receiver (RX). By using the transmitter and receiver, a 100-Gb/s quantum stream cipher transmission is introduced in an amplifier repeated fiber link of 120 km.

II. Y-00 Quantum Stream Cipher

Y-00 is a physical cipher and has the potential that realizes the provable security level based on physical complexity, and features high compatibility with the current optical fiber communication systems. In general, the process to break the secret key or the information from the ciphertext consists of two steps. The first step is to read the ciphertext correctly. The second is the ciphertext is processed mathematically to recover the secret key/the plaintext, i.e., the original information before encryption. Y-00 makes the first step difficult by multi-level encryption of basis that sends the binary data.

Figure 1 compares the conventional cipher and the Y-00. In general, the conventional cipher based on the mathematical encryption converts binary data of plaintext into binary data of ciphertext. Therefore an attacker can discriminate the two correct signal levels, "0" and "1", of the ciphertext, and he can

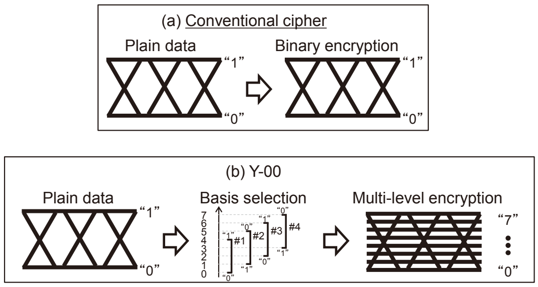


Fig.1. Comparison of (a) conventional cipher and (b) Y-00 (basis M = 4).

succeed in acquiring the ciphertext. On the other hand, in Y-00, the binary data is encrypted thorough the multilevel encryption by using the sets of basis. Thus, the security level of the Y-00 is higher than that of the mathematical cipher, and is measured by the physical complexity based on the masking. This is the new concept in cryptology. It should be noted the legitimate user who has the secret key knows the basis of each signal and he can process the observed Y-00 signal to recover the original information just by the binary detection.

According to the theoretical research results, the randomization of encrypted data (ciphertext) by quantum noise at detection of an eavesdropper who tries to break the cipher is one of the significant parameters for evaluating the security level of Y-00. The authors experimentally observed the amount of the randomization that was sufficient for the practical use [8].

III. Configuration of Transmitter and Receiver

Figure 2 (a) is a block diagram showing basic functions of a transmitter (TX) and a receiver (RX) for Y-00 protocol. Schematic waveforms in main parts are illustrated. A running key is generated in a PRNG from a seed key, which is shared in the TX and RX. Currently, a linear feedback shift register is employed as a PRNG and the key length of the seed key is extended. In an overlapped selection keying (OSK) based on XOR operation between input binary data (Fig.2 (b)) and the running key, the polarity of the 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 log2M (M: number of basis level) of the PRNG output is produced in the M-ary circuit. Next the block signal is scrambled by a mapper. The scrambled input binary data are modulated by the running key in a bit-by-bit manner to generate multi-level electrical signals. An intensity of a light is modulated by the electrical signals with a bias voltage to induce optical offset. In this way, multi-level optical signals (Fig.2 (c)) are generated. In the receiver, first, Y-00 signals are converted to electrical signals by direct detection. Then, basically, the inverse procedure used in the TX demodulates to restore the original binary signal (Fig.2 (d)) by using the seed key. Please note that clock signal is recovered from the Y-00 signal although the function is not shown in the schematic.

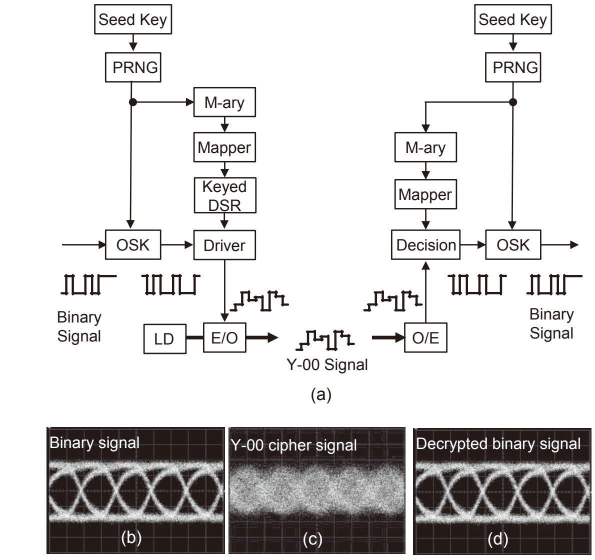


Fig. 2. (a) Schematic of Y-00 transmitter and receiver. Waveforms of (b) binary signal, (c) Y-00 cipher signal and (d) decrypted binary signal

IV. 100-Gbit/s Y-00 Cipher Transmission Experiment

Experimental setup is shown in Fig.3 (a). Lights of 10 CW laser diodes (LDs) with a wavelength spacing of 50 GHz (0.4 nm) from ch.1:λ = 1549.7 nm to ch.10:λ = 1553.3 nm were multiplexed and modulated with an intensity modulator by 10-Gb/s 64 level electrical signals generated from basis selection signals generated from a seed key of 128 bit and also binary data of pseudo-random bit sequence (PRBS) of 2^{31}-1, generating 100-Gb/s WDM Y-00 signals. The detail of the 10-Gb/s Y-00 TX and RX is described in [13]. The 120-km transmission line consisted of three sets of a 40-km long dispersion shifted fiber and an optical amplifier. The input power to each fiber was set to -1 dBm/wavelength. In the receiver, after demultiplexing in wavelength and O/E conversion by the direct detection, a clock signal was recovered. By using the basis selection signals generated from the shared key, the intensity threshold set in a bit-by-bit manner and binary signals were obtained.

Figure 3(b) shows the optical spectrum measured at the receiver end. Optical SNRs of all channels were over 30 dB/0.1nm. A waveform of 10-GHz recovered clock is shown in Fig.4(a). The recovered clock was used for a trigger of waveform measurements and bit error rate (BER) measurements. The jitter of the recovered clock was calculated from the single-sideband phase noise shown in Fig.4(b). It was 1.3 ps and low enough for measurements of 10-Gb/s signals. The waveforms of all channels of Y-00 signals and corresponding signals decrypted with the seed key were measured. The waveforms of all channels were similar,

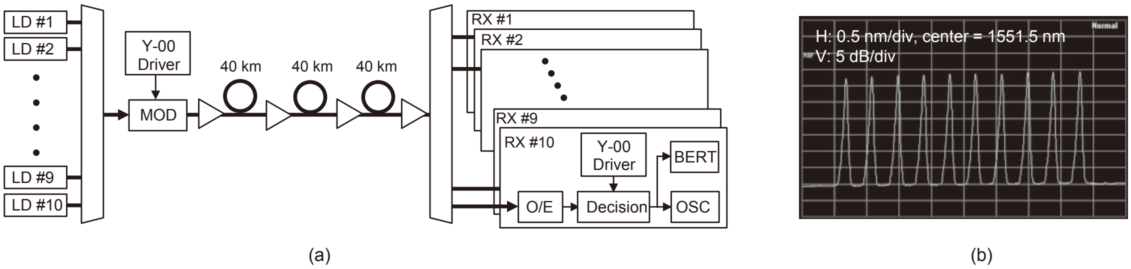
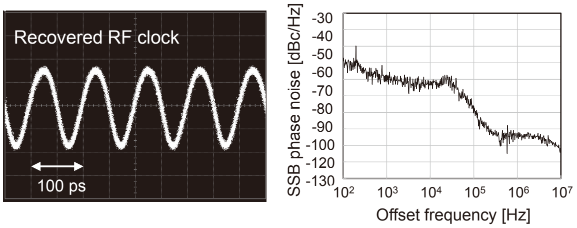


Fig. 3. (a) Experimental setup. (b) Optical spectrum measured after 120-km transmission.



(a) (b)

Fig.4. (a) Waveform and (b) single-sideband phase noise of recovered 10-GHz clock.

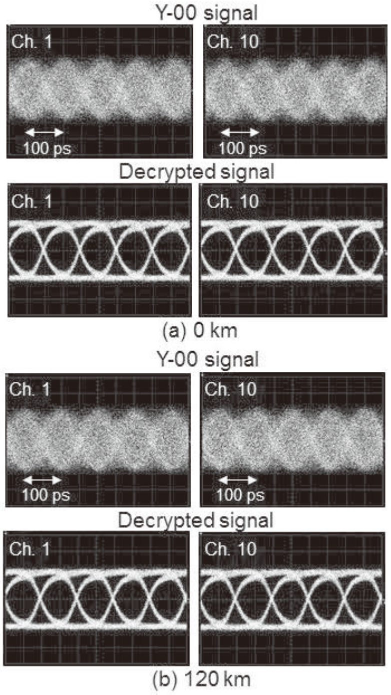


Fig. 5. Waveforms of Y-00 signals (Ch.1 and Ch.10) and corresponding decrypted binary signals at (a) 0 km, and (b) 120 km.

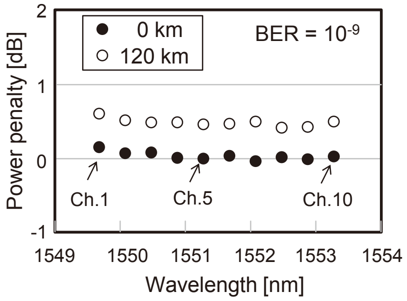


Fig.6. Power penalties of 10 channels at BER = 10^{-9}

therefore, as examples, waveforms of ch.1 and ch.10 are shown in Fig.5. While eye-openings of Y-00 signals (Fig.5 (a)) were not observed due to intensity noise even at the TX (0 km), eye-openings of the decrypted binary signal were clearly measured. The signals measured at TX are shown in Fig.5 (b). Binary signals after decryption showed clear eye-openings. BERs of the decrypted binary signals for all ten channels were measured to confirm all channels achieved BERs < 10^{-9}. Power penalties defined as a relative power to the power of ch.5 for achieving BER = 10^{-9} at TX and RX are summarized in Fig.6 by closed circles and open circles, respectively. The power penalties were less than 0.7 dB for all channels. It should be noted that the transmission distance was limited by the number of available transmission fibers and optical amplifiers. The capacity was experimentally limited by number of LDs we have. The theoretical capacity increase was discussed in [14].

V. Conclusion

For realizing high capacity optical data link with a secure function to protect eavesdropping, we have achieved 100-Gb/s Y-00 cipher transmitter and receiver with 64-level intensity modulation. The capacity has been increased by multiplexing 10 wavelengths each carrying 10-Gb/s data. The 100-Gb/s Y-00 cipher has been successfully transmitted over a 120-km optical link composed of three spans of a 40-km optical fiber and an amplifier. The authors believe Y-00 quantum stream cipher is useful for secure and high capacity optical data link.

Acknowledgment

This work was supported in part by Fujitsu Laboratories Ltd and the Telecommunications Advancement Foundation.

References

[1] DARPA, "Quiness: Macroscopic Quantum Communications," Solicitation Number: DARPA-BAA-12-42,https://www.fbo.gov/index?s=opportunity&mode=form&id=6a3a61d577305f71d9be268925c4b201&tab=core&tabmode=list&=

[2] K. Guan, P. J. Winzer and E. Soljanin, "Information-theoretic security in space-division multiplexing fiber optic networks," in Proc. ECOC, Tu.3.C4, 2012.

[3] G. D. Crescenzo, R. Menendez, and S. Etemad, "OCDM-based photonic encryption with provable security," in Proc. OFC, OTuP3, 2008.

[4] G. Cincotti, N. Wada, and K. Kitayama, "Secure optical bit- and block-cipher transmission using a single multiport encoder/decoder," in Proc. OFC, JThA93, 2008.

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

[6] 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.

[7] O. Hirota, "Cyber attack against optical communication systems and its defense technology, - toward development of Quantum Enigma Cipher -," IEICE Technical report OCS2013-18, pp.43 - 48, June 2013.

[8] F. Futami and O. Hirota, "Masking of 4096-level intensity modulation signals by noises for secure communication employing Y-00 cipher protocol," in Proc. ECOC, Tu.6.C.4, 2011.

[9] F. Futami and O. Hirota, Field transmission test of 2.5 Gb/s Y-00 cipher in 160-km (40 km × 4 spans) installed optical fiber for secure optical fiber communications, Proc. 11th International Conf. on Quantum Comm. Measurement and Computing (QCMC2012), P1-38, 2012.

[10] F. Futami and O. Hirota, "40 Gb/s (4 × 10 Gb/s) Y-00 protocol for secure optical communication and its transmission over 120 km," in Proc. OFC, OTu1H.6, 2012.

[11] K. Kato and O. Hirota, "Quantum quadrature amplitude modulation system and its applicability to coherent state quantum cryptography," SPIE conference on quantum communication and imaging III. SPIE Proc. vol-5893, 2005.

[12] M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai., "QAM quantum stream cipher using digital coherent optical transmission," Opt. Express 22, pp.4098-4107, 2014.

[13] K. Ohhata, O. Hirota, M. Honda, S. Akutsu, Y. Doi, K. Harasawa, and K. Yamashita, "10-Gb/s optical transceiver using the Yuen 2000 encryption protocol," J. of Lightwave Technol. vol. 28, no. 18 , pp.2714-2723, 2010.

[14] F. Futami, M. Soma, K. Kato, and G. Masada, "WDM transmission experiment of Y-00 stream cipher and study on transmission capacity enhancement by multiplexing technique," Tamagawa University Research Review, No.18, pp.53-60, 2012.