ISSN 2186-6570

Conversion performance investigation of Y-00 quantum stream cipher transceiver between GbE signals and Y-00 cipher signals

Fumio Futami, Ken Tanizawa, and Kentaro Kato

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

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.7, No.1, 29-31, 2017

Conversion performance investigation of Y-00 quantum stream cipher transceiver between GbE signals and Y-00 cipher signals

Fumio Futami, Ken Tanizawa, and Kentaro Kato
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 realizing secure physical layer of optical fiber communications using physical cipher, we developed a Y-00 quantum stream cipher transceiver that connects GbE signals to Y-00 cipher signals. So far, we focused on investigations of secure optical fiber transmission using the Y-00 quantum stream cipher transceiver. In this work, we experimentally investigate conversion performance of the Y-00 transceiver between GbE signals and Y-00 cipher signals, and it is confirmed that full data rate of 1000 Mbit/s is achieved. In addition, we construct a GbE full duplex communication system where GbE signals are converted to Y-00 signals by Y-00 transceivers and secure communication is realized. In the system, actual data files of video clips is successfully transferred, and also full HD video streaming is successfully demonstrated.

***Index Terms*— Y-00 quantum stream cipher, physical cipher, GbE protocol, secure optical communication.**

I. Introduction

Secure data transmission technology in the physical layer of optical transmission system is expected since data in transmission today may contain sensitive information. Currently, optical fiber transmission technology generally offers communications of high capacity and long transmission distance. A new function of high security can be added to the transmission system when we employ physical cipher, which features the use of physical phenomenon, in the physical layer. Aiming at offering a function of high security, we have been engaged in the research and development of practical physical cipher whose security relies on the physical effect.

Y-00 quantum stream cipher or simply Y-00 cipher is noise-based physical layer encryption. It employs dense multi-level modulation, which requires no excess bandwidth. No new device development is required, but it is implemented with readily available 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. Y-00 cipher is realized by modulation schemes such as multi-level phase modulation (PSK) [1], intensity modulation (ISK) [2] and quadrature amplitude modulation (QAM) [3,4]. So far, we demonstrated ISK Y-00 at 2.5 Gbit/s by using 4096-intensity level signals [5,6]. The highest capacity we achieved so far was 100 Gbit/s [7]. Recently, for practical use, we developed a Y-00 quantum stream cipher transceiver using 4096-intensity levels [8]. Irregular mapping and overlap selection keying (OSK) as randomization scheme [9] is incorporated in the Y-00 transceiver for realizing higher security. So far, performance of secure transmission and the irregular mapping were experimentally investigated. The Y-00 transceiver is designed to be capable of conversion between Y-00 cipher signals and GbE signals. GbE can handle data rate of 1000 Mbit/s (125 Mbyte/sec). However, we have never investigated conversion performance between Y-00 signals and GbE signals.

In this work, we focus on investigation of conversion performance of the Y-00 transceiver. First, we experimentally measure conversion rate using GbE frame generated by a GbE signal quality analyzer where pseudo random bit sequence (PRBS) is set to the payload of GbE frame, and conversion rate of 1000 Mbit/s is successfully confirmed. Next, instead of artificial data, actual data files of video clips are transferred from a personal computer to a network attached storage using Y-00 cipher transceivers, and a video clip with file size of 1 Tbytes is successfully transferred. Finally, a streaming of compressed full HD video is successfully demonstrated using the Y-00 transceivers.

II. Measurements of Conversion Rate

An experimental setup for measuring conversion rate of the Y-00 transceiver is shown in Fig.1. It consists of a GbE signal quality analyzer and two Y-00 transceivers, #1 and #2. The two transceivers are the same specification and share the same key. The Y-00 transceiver connects GbE signals to Y-00 signals in

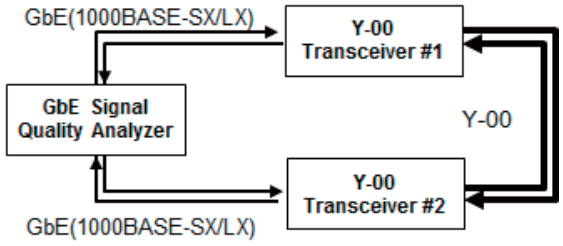

Fig.1. Experimental setup for measuring the conversion speed of Y-00 transceiver in full duplex GbE communication.

Fig.2. A photo of Y-00 quantum stream cipher transceiver.

the full duplex communication. Figure 2 is a photo of the Y-00 quantum stream cipher transceiver. Its size is 19-inch wide with the height of 1U (= 44 mm). The Y-00 interface is the SC-type connector, and the interface for GbE supports SFP (Small Factor Pluggable). Two transceivers were directly connected by a couple single mode fibers for the full duplex communication. The input power to the transceiver was set to -10 dBm. The wavelength of Y-00 cipher signals was set to 1550.12 nm and the number of multi-level intensity signals was set to 4096 (12 bit). The binary data of GbE is encrypted thorough 4096-level Y-00 cipher signals by using the sets of basis the shared key generated. For decryption, 4096-level Y-00 cipher signal is converted to binary GbE signal using the same sets of basis. The signal analyzer has SFP module interfaces and each SFP was connected to a Y-00 transceiver with a couple of optical fibers. The GbE signal quality analyzer generates and receives Ethernet

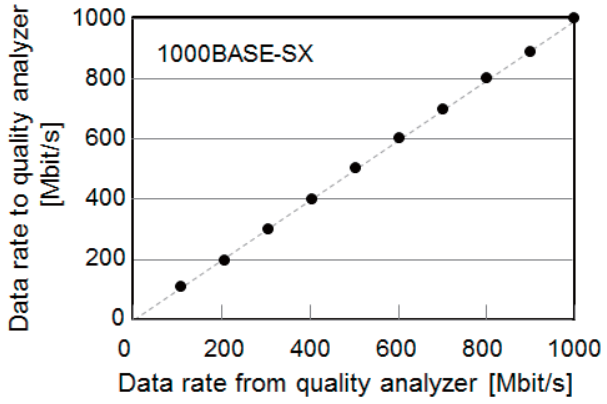

Fig. 3. Conversion speed of the Y-00 transceiver when a SFP optical module of 1000BASE-SX is plugged in the GbE interface of the Y-00 transceiver.

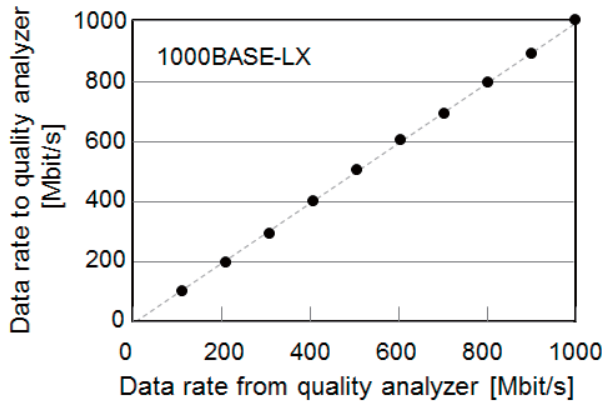

Fig. 4. Conversion speed of the Y-00 transceiver when a SFP optical module of 1000BASE-LX is plugged in the GbE interface of the Y-00 transceiver.

frames, and analyzes input/output characteristics of the Ethernet frames.

In the measurements, the data rate of Ethernet frames generated from the analyzer was adjusted by changing the inter frame gap of Ethernet frames. A pseud random bit sequence (PRBS) is loaded as data in the payload of the Ethernet frame. Frame lengths were set to have random lengths from 64 byte to 1518 byes. Two kinds of SFP modules, 1000BASE-SX and 1000BASE-LX, were tested. First, for test purpose, the transfer rate with no Y-00 transceivers was measured by directly connecting two SFP modules in the quality analyzer with a couple of optical fibers. The maximum transfer speed was verified to be 1000 Mbit/s for 1000BASE-SX and 1000BASE-LX. Next, conversion rates were measured when 1000BASE-SX operating in near infrared (NIR) wavelength was used for connections with the analyzer and Y-00 transceivers. The data rates of the downstream and upstream were exactly the same as the data rate from the quality analyzer as shown in Fig.3. From the measurement results, the maximum load capacity of the Y-00 transceiver was confirmed to be 1000 Mbit/s. Next, the SFP modules were exchanged to 1000BASE-LX operating at the wavelength of 1.3 μm range. The measurement results are shown in Fig.4. Data rate of 1000 Mbit/s was also achieved when the SFP optical module of 1000BASE-LX was utilized.

III. Secure Transfer of Actual Data File

In the previous section, the conversion speeds of the Y-00 transceivers were experimentally measured using PRBS in the payload of the Ethernet frame. In this section, transfer of actual data instead of artificial data was demonstrated in a full duplex GbE communication system experimentally constructed, and transfer rate of real data was measured. The experimental system is composed of two Y-00 transceivers, two media converters, a personal computer and a network attached storage (NAS) as shown in Fig.5. The media converter transparently connected 1000BASE-LX to 1000BASE-T. Here, we employ video clip files as real data and measured copy time. Figure 6 shows the copy times and copy speeds when data was copied from the PC

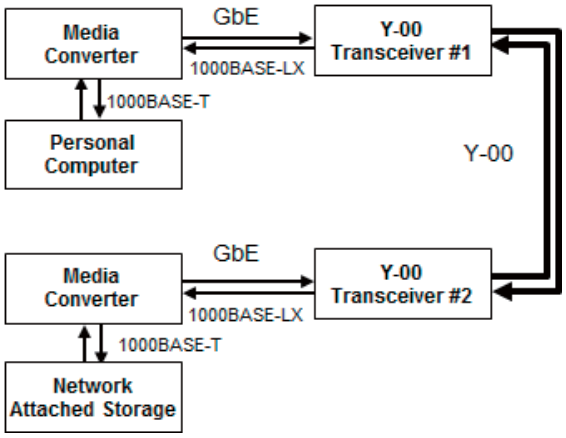

Fig.5. Experimental setup for copying actual data files of video clip using Y-00 transceiver and media converter in a full duplex GbE communication system.

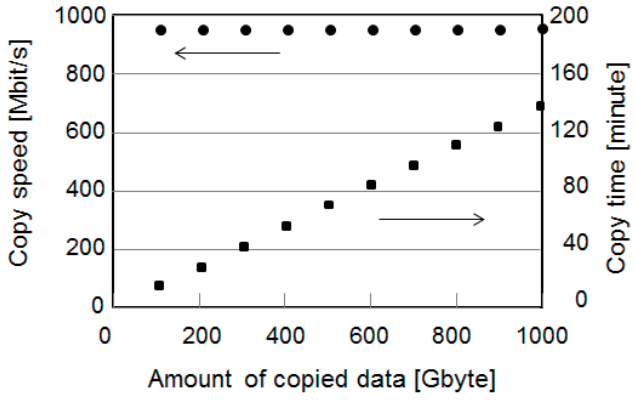

Fig. 6. Copy speed and copy time when actual data of video clips are transferred to a network attached storage (NAS). The speed was mainly limited by the writing speed to the NAS.

by a copy command in Window operating system. A video clip file of 1-Tbytes (8 Tbits) data was copied in about 140 minutes. The speed was about 946 Mbit/s, although the Y-00 transceiver has capability to handle data speed of 1000 Mbit/s as experimentally demonstrated in the previous section. A reason not to achieve 1000 Mbit/s was the writing speed limitation to NAS.

IV. Video Streaming Experiment

Finally, a streaming of a full HD video was demonstrated using Y-00 transceivers in the setup shown in Fig. 7. The video compressed in the full HD camcorder was output to HDMI interface. The data rate of the full HD after compression was about 10 Mbit/s. The HDMI signal was converted to Ethernet frame by a HDMI-GbE encoder, and then the Ethernet frames was input to a Y-00 transceiver. The video data was securely delivered to a second Y-00 transceiver by Y-00 cipher signals. The second transceiver decrypted to Ethernet frame and the video data was decoded to HDMI signal by a GbE/HDMI decoder. The video after transmission was successfully projected on a display.

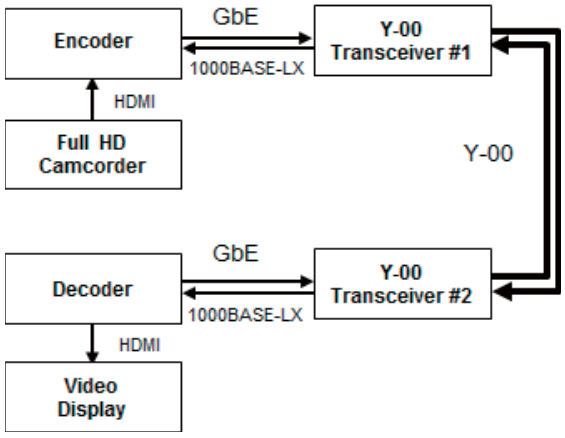

Fig.7. Experimental setup for a streaming of a full HD video using Y-00 transceiver and HDMI-GbE encoder/decoder in a full duplex GbE communication system.

V. Conclusion

In this work, investigation of conversion performance of the Y-00 quantum stream cipher transceiver between GbE signals and Y-00 signals have been focused on. First, we have experimentally measured conversion rates using GbE frame generated by a GbE signal quality analyzer where pseud random bit sequence (PRBS) are loaded in the payload of GbE frame, and conversion rates of 1000 Mbit/s has been confirmed. Next, instead of artificial bit sequence, actual data files of video clips have been transferred from a personal computer to a network attached storage (NAS) using Y-00 cipher transceivers in the full duplex GbE communication system, and a video clip of 1-Tbytes file size has been successfully copied in the NAS. Finally, a streaming of a full HD video has been successfully demonstrated using the Y-00 transceivers.

References

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

[2] 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.

[3] 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.

[4] 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..

[5] 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.

[6] 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.

[7] F. Futami, and O. Hirota, "100 Gbit/s (10 × 10 Gbit/s) Y-00 cipher transmission over 120 km for secure optical fiber communication between data centers," Proc. OECC/ACOFT2014, MO1A2, (2014).

[8] F. Futami, K. Kato, and O. Hirota, "A novel transceiver of the Y-00 quantum stream cipher with the randomization technique for optical communication with higher security performance," Proc. SPIE 9980, 99800O (2016)

[9] K. Kato, and O. Hirota, "Randomization techniques for the intensity modulation-based quantum stream cipher and progress of experiment", Proc. SPIE 8163, 81630A (2011)