ISSN 2186-6570

Investigation of Error Correction Performance using Reed-Solomon Code for GbE Packet in Y-00 Quantum Stream Cipher Transceiver

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.8, No.1, 17-19, 2018

Investigation of Error Correction Performance using Reed-Solomon Code for GbE Packet in Y-00 Quantum Stream Cipher Transceiver

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*—**

Error correction code reduces errors in data by encoding the message with a redundant. The Reed-Solomon code is a block-based error correction code applicable to digital optical communications. A function of error correction (EC) using Reed-Solomon code is installed in Y-00 cipher packets of a Y-00 quantum stream cipher transceiver operating for GbE packets. In this work, we focus on experimental investigation of the error correction performance when noise is added to Y-00 cipher signals. First, bit error ratios (BERs) of binary data in a payload of a GbE frame are measured, and optical signal-to-noise ratio (OSNR) gain of more than 10 dB is achieved by EC at BER of 10^{-9}. Next, loss ratios of GbE packets are measured, and OSNR required for the packet loss of 10% is decreased owing to EC operation.

***Index Terms*— Error correction, Reed-Solomon code, Y-00 quantum stream cipher, physical cipher, GbE protocol, secure optical communication.**

I. Introduction

Security of the net has got lots of attention recently since we sometimes transmit sensitive data over the net. The physical layer, i.e., the transport layer, is the only layer that a physical phenomenon can be applied to offer a function of the security in the digital communication system. Physical cipher using such phenomena can offer higher security when it is employed with the mathematical cipher that relies on a mathematical algorithm for encryption and decryption. Y-00 quantum stream cipher [1-6] is physical cipher that makes use of randomness generated by a combination of the mathematical encryption and a physical phenomenon. Aiming at offering a function of high security, we have been engaged in the research and development of Y-00 cipher. Among several modulation schemes of Y-00 cipher, intensity modulation features simple modulation and detection. For the purpose of evaluating both communication and security performance of Y-00 cipher, we fabricated a transceiver of Y-00 quantum stream cipher [7] in which randomization technique of an irregular mapping and overlap selection keying were implemented for enhancing the security [8, 9]. The Y-00 cipher transceiver is designed for operating for Gigabit Ethernet (GbE) protocol. A GbE packet and Y-00 cipher packet are interconverted in the transceiver. The transceiver successfully applied to secure communications such as a point-to-point transmission [7], an overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system [10]. Secure networking was also demonstrated using an optical switch in a node of a network deployed in the downtown of Tokyo [11]. An experimental security investigation of Y-00 cipher has been also demonstrated, and an amount of noise masking representing a ratio of a noise amount to a minimum signal distance was also experimentally measured [12-14].

An error correction (EC) function is installed in the Y-00 cipher transceiver for improving transmission performance. As described in the next section, a Y-00 packet is encoded and decoded by the Reed-Solomon code. In this work, we investigate performance of error correction of Reed-Solomon code in the Y-00 quantum stream cipher transceiver. First, bit error ratios (BERs) of a payload of a GbE frame after decryption are measured when noise is added to Y-00 cipher signals. An optical signal-to-noise ratio (OSNR) gain of more than 10 dB is achieved by EC at BER of 10^{-9}. Next, loss ratios of GbE packets are measured, and OSNR required for the loss of 10% is decreased owing to EC operation.

II. Encoding and Decoding using Reed-Solomon Code

In a transmitter part of Y-00 cipher transceiver, an incoming GbE packet from a small form-factor pluggable (SFP)

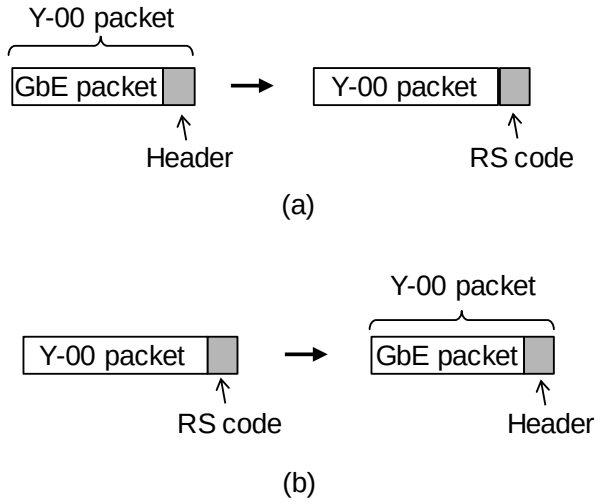

Fig.1. Schematic of Y-00 packets of (a) Encoding and (b) decoding using error correction by the Reed-Solomon code.

transceiver is converted to a Y-00 packet with a header. Then error correction code of the Reed-Solomon code is added to the packet as an overhead. Coding overhead is 7.1 %. In a receiver part of Y-00 cipher transceiver, a Y-00 packet with error correction code is decoded and a Y-00 packet is obtained. Then, the Y-00 packet is converted back to a GbE packet which is output to a transmitter of a SFP transceiver.

III. Measurements of BER with Error Correction

Error correction performances by the Reed-Solomon code are measured. A pseudo-random bit sequence (PRBS) is loaded as binary data in a payload of an Ethernet frame and BERs of the data are measured when EC is turned on and off. Figure 2 shows an experimental setup where two Y-00 cipher transceivers are connected by an optical fiber. White Gaussian noise from a noise source with a bandwidth of 0.5 nm is added to a Y-00 cipher signal from the transceiver #1 for varying a Y-00 signals of OSNR to the transceiver #2. A 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 details of the transceiver is described in Ref.[7]. An OSNR of the signal launched into the transceiver #2 is measured by an optical spectrum analyzer. Measurement results are shown in Fig. 3. The OSNR required for BER = 10^{-9} are 30 dB when EC is disabled while 19 dB is required when EC is enabled. An EC

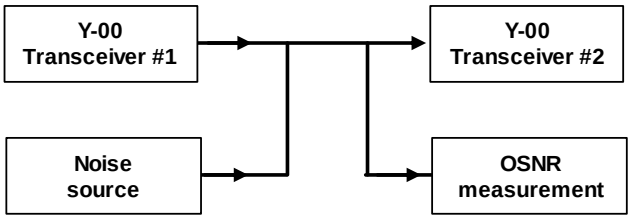

Fig.2. Experimental setup for measuring BER with and without error correction. Noise from a noise source is added to vary signal quality.

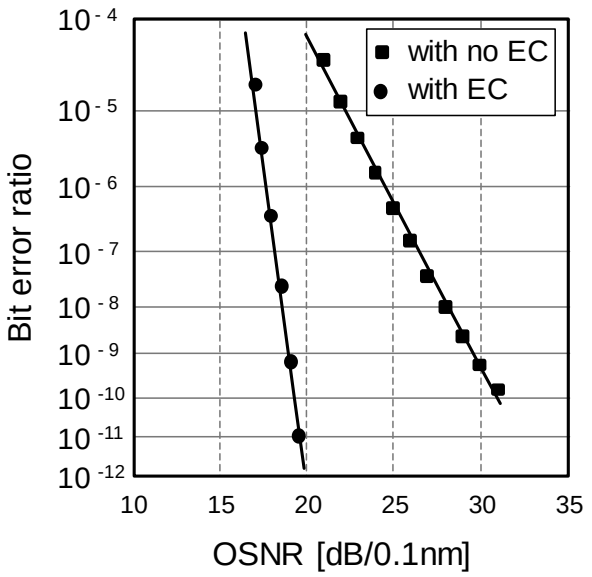

Fig. 3. BERs of PRBS in a payload of GbE packet.

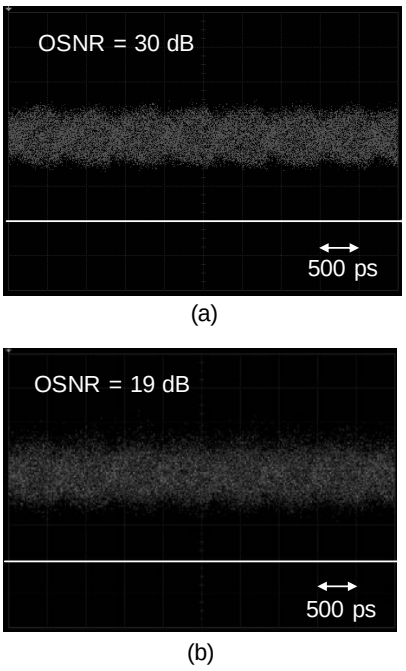

Fig. 4. Sampling waveform of Y-00 cipher signals. (a) OSNR = 30 dB when BER is about 10^{-9} is achieved with no EC, and (b) OSNR = 19 dB when BER is about 10^{-9} is achieved with EC. The white line shows the zero level.

gain is about 10 dB. Sampling waveforms are measured by using a DC-coupled photo-detector with a bandwidth of 12.4 GHz. Compared with a sampling waveform of a Y-00 cipher signal with OSNR = 30 dB as shown in Fig. 4(a), a sampling waveform of a Y-00 cipher signal with OSNR = 19 dB (Fig.4(b)) has much more noise. However, the same BER of 10^{-9} is achieved with both Y-00 cipher signals when EC is enabled for the Y-00 cipher signal with lower OSNR.

IV. Measurements of Loss Ratio of GbE Packet

A loss ratio of GbE packets are also investigated experimentally when EC is enabled and disabled. Figure 5 shows a schematic of an experimental setup. A GbE packet from a GbE generator is launched into a receiver of a SFP transceiver of 1000BASE-LX plugged to a SFP port of the Y-00 transceiver #1. Then the GbE packet is framed to a Y-00 packet and encoded by RS code. After that, the Y-00 packet is optically transmitted to the Y-00 transceiver #2. In the transceiver #2, the GbE packet is recovered from the Y-00 packet after EC is performed. Finally, the GbE packet is sent to the GbE counter and the number of GbE packets that are correctly received are counted. In the measurements, the data rate of Ethernet packet generated from the generator is adjusted by changing the inter-frame gap of Ethernet packets. A 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 byte.

A number of GbE packet is measured in the counter by changing an amount of noise added to a signal carrying the Y-00 packet when EC is turned on and off. A packet loss ratio is calculated by the number of GbE packets sent from the

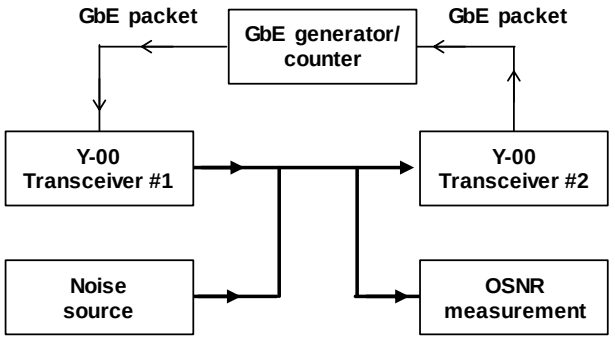

Fig.5. Experimental setup for measuring GbE packet loss ratios with and without error correction. Noise from a noise source is added to vary signal quality.

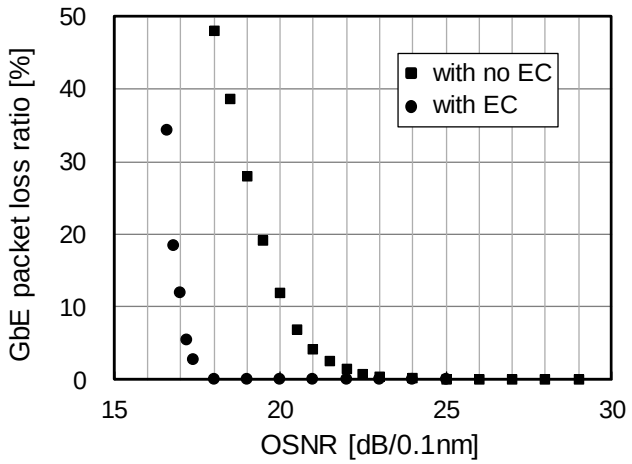

Fig. 6. GbE packet loss ratio with error correction (●), and without error correction (■).

generator and the number of GbE packets measured with the counter. Figure 6 shows GbE packet loss ratios with and without EC. An OSNR required for the loss ratio of 10% is more than 3-dB lower when EC is performed. A loss ratio of 48% with no EC is suppressed to almost 0% with EC at OSNR of 18 dB.

V. Conclusion

Performance of an error correction function in the Y-00 quantum stream cipher transceiver has been experimentally investigated. The Reed Solomon code of the error correction function has been implemented for improving communication performance of the Y-00 cipher of the transceiver. Coding overhead of the error correction has been set to 7.1 % and communication performance has been improved when the error correction has been applied. First, bit error ratios of a payload of a GbE frame after decryption have been experimentally measured when white Gaussian noise is added to Y-00 cipher signals, and an OSNR gain of more than 10 dB has been achieved by the error correction at bit error ratio of 10^{-9}. Next, loss ratios of GbE packets have been measured using a GbE packet generator and counter. The OSNR is decreased by about 3 dB owing to the error correction when the loss ratio of GbE packet is 10%. In addition, a loss ratio at an OSNR of 18 dB has been suppressed to almost 0 % after EC has been applied while it was 48% with no EC.

References

[1] H. P. Yuen, “KCQ: A new approach to quantum cryptography I. General principles and key generation,” https://arXiv:quant-ph/0311061v6.

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

[3] K. Tanizawa, and F. Futami, “Digital Coherent Detection with Decryption in PSK Y-00 Quantum Stream Cipher,” The 23rd Opto-Electoronics and Communication conference (OECC 2018), 5D1-1, 2018.

[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] 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.

[6] 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.

[7] 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)

[8] T. Shimizu, O. Hirota, and Y. Nagasako, “Running key mapping in quantum stream cipher by Yuen 2000 protocol,” Phys. Rev. A ,77, 034305, (2008).

[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)

[10] F. Futami, K. Guan, J. Gripp, K. Kato, K. Tanizawa, S. Chandrasekhar, and P. J. Winzer, “Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system,” Optics Express 25(26), 33338-33349 (2017)

[11] F. Futami, T. Kurosu, K. Tanizawa, K. Kato, S. Suda, and S. Namiki, “Dynamic Routing of Y-00 Quantum Stream Cipher in Field-Deployed Dynamic Optical Path Network,” Proc. Optical Fiber Communication Conference (OFC 2018), Tu2G.5, (2018)

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

[13] F. Futami, K. Tanizawa, K. Kato, and O. Hirota, “Experimental investigation of security parameters of Y-00 quantum stream cipher transceiver with randomization technique: part I”, Proc. SPIE 10409, 104090I (2017)

[14] F. Futami, K. Tanizawa, K. Kato, and O. Hirota, “Experimental investigation of security parameters of Y-00 quantum stream cipher transceiver with randomization technique: part II”, Proc. SPIE 10771, 1077114, (2018)