ISSN 2186-6570

Digital-Coherent Detection of PSK Y00 Quantum-Noise Randomized Stream Cipher Signal

Ken Tanizawa, 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.7, No.1, 1-4, 2017

Digital-Coherent Detection of PSK Y-00 Quantum-Noise Randomized Stream Cipher Signal

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

Abstract—

We report digital feedforward carrier phase estimation (CPE) for coherent detection of phase-shift keying Y-00 quantum-noise randomized stream cipher signal. The feedforward CPE is equipped with Y-00 decryption process in a digital domain. Numerical simulations show that the feedforward CPE with decryption process tracks phase noise of a laser and achieves penalty-less coherent detection.

***Index Terms*— Y-00 quantum stream cipher, digital-coherent transmission, secure fiber-optic communication system.**

I. Introduction

Fiber-optic transmission faces a potential threat of eavesdropping, and its security is increasingly important recently. An approach to protect fiber-optic transmission from such a threat is to use a symmetric-key direct data encryption in a physical layer. Particularly, Y-00 quantum-noise randomized stream cipher technology [1] is promising since it provides not only provable security against various attacks [2] but also high compatibility with modern fiber-optic networks where data rate per channel is over Gbit/s [3],[4]. In Y-00 signal transmission, legitimate users who share keys exchange ciphertext masked by quantum noise. Masking of the data, or Y-00 encryption, is implemented with multi-level modulation of phase [5],[6], intensity [7],[8], or quadrature amplitudes [9],[10].

Recently, unified analysis of these modulation formats for Y-00 encryption was reported [11]. The encryption based on phase modulation requires higher modulation multiplicity than the one in the intensity modulation for the same level of security. On the other hand, in terms of transmission performances such as receiver sensitivity and spectral efficiency, phase-shift keying (PSK) Y-00 signal has advantages since coherent detection is employed. We focus on PSK Y-00 signal in this paper. PSK Y-00 signal transmission was studied in the early stage of researches on Y-00 quantum stream cipher technology [5],[6]. Transmission experiments at an OC-12 data rate were demonstrated [6]. In the setup, Y-00 decryption was achieved in an optical domain with a phase modulator, and analog (differential) coherent detection using a 1-bit delay interferometer was employed.

In the past decade, for conventional non-cipher PSK signals, digital-coherent detection becomes widely used. Carrier phase estimation (CPE) which tracks phase noise of received signal [12] and compensation of linear distortion caused by transmission over optical fibers [13] are achieved stably in a digital domain, which contributes to high data-rate and long reach transmission. Targeting digital-coherent detection of PSK Y-00 signal, we propose a digital feedforward CPE that incorporates decryption process in a digital domain [14]. To extract phase noise, data modulation is canceled by calculating an Mth power of a complex amplitude of decrypted signal. This paper details digital-coherent detection using the feedforward CPE with decryption process. Numerical simulations show that 10-Gbaud PSK Y-00 signal is successfully demodulated with the feedforward CPE. A possible digital-coherent detection scheme using a feedforward CPE without decryption process is also discussed.

II. Digital Coherent Detection of PSK Y-00 Signal

Multi-level phase modulation is employed for the generation of PSK Y-00 signal. Fig. 1 shows the mapping of Y-00 signal in an I-Q plane, when the data modulation is binary PSK. The phase of the signal is modulated to 0 or π by binary data. At the same time, the basis of the phase modulation is selected between 0 to π in a symbol-by-symbol manner for the encryption. The total phase of the Y-00 signal is expressed as

$$\theta_{\mathrm{Y00}}(t) = \theta_{\mathrm{data}}(t) + \theta_{\mathrm{basis}}(t) + \theta_{\mathrm{sn}}(t) \qquad (1)$$

where $\theta_{\mathrm{data}}(t)$ and $\theta_{\mathrm{basis}}(t)$ are the phases of the data and basis modulations, respectively, and $\theta_{\mathrm{sn}}(t)$ is the phase noise of the signal. A mathematical encryption box generates the random basis using keys shared between legitimate users. The number of bases N_{basis} should be large, which makes the distance between adjacent bases very short. Provided that the distance is less than the standard deviation of shot noise, strong data masking, assisted by the quantum nature, is achieved. The electrical field of the PSK Y-00 signal $E_{\mathrm{Y00}}(t)$ is written as

$$E_{\mathrm{Y00}}(t) = A_{\mathrm{s}}(t)\exp\{j(\theta_{\mathrm{Y00}}(t) + \omega_{\mathrm{s}}t)\} \qquad (2)$$

where $A_{\mathrm{s}}(t)$ is the amplitude, and ω_{s} is the angular frequency of the signal.

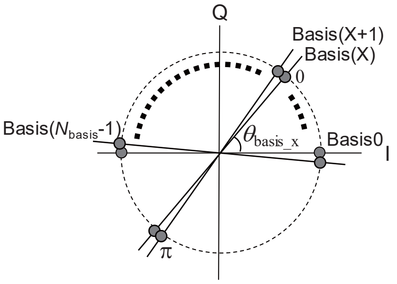

Fig. 1. Mapping of PSK Y-00 signal.

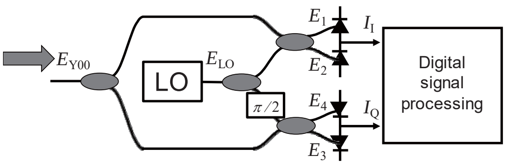

Fig. 2. Configuration of a digital-coherent receiver.

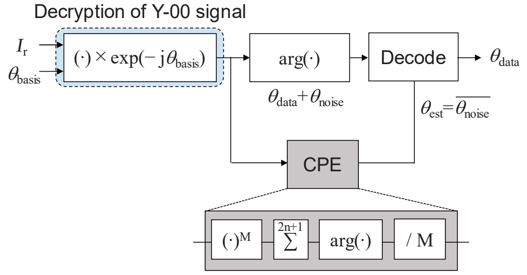
Decryption of Y-00 signal
I_{r}
θ_{basis}
$(\cdot)\times\exp(-j\theta_{\mathrm{basis}})$
arg(·)
Decode
θ_{data}
$\theta_{\mathrm{data}}+\theta_{\mathrm{noise}}$
$\theta_{\mathrm{est}}=\overline{\theta_{\mathrm{noise}}}$
CPE
$(\cdot)^M$
2n+1 Σ
arg(·)
/ M

Fig. 3. Block diagram of the digital signal processing for CPE with Y-00 decryption process.

Coherent detection of PSK Y-00 signal is achieved with a phase-diversity homodyne coherent receiver [15]. Fig. 2 shows the configuration. It consists of a local laser, a 90-degree optical hybrid circuit and two balance photo detectors. The electrical fields of the Y-00 signal and continuous-wave local oscillator, $E_{\mathrm{Y00}}(t)$ and E_{LO}, are mixed at the 90-degree optical hybrid circuit. Then, mixed electrical fields, E_1, E_2, E_3, and E_4, are launched into the balance photo detectors. Two output photocurrents from the detectors are given as

$$I_{\mathrm{I}}(t) = R\sqrt{P_{\mathrm{s}}(t)P_{\mathrm{LO}}}\cos\left(\theta_{\mathrm{Y00}}(t)-\theta_{\mathrm{LO}}(t)\right) \tag{3}$$

$$I_{\mathrm{Q}}(t) = R\sqrt{P_{\mathrm{s}}(t)P_{\mathrm{LO}}}\sin\left(\theta_{\mathrm{Y00}}(t)-\theta_{\mathrm{LO}}(t)\right) \tag{4}$$

where R is the responsivity of the photodiode, $P_{\mathrm{s}}(t)$ and P_{LO} are the powers of the signal and local oscillator, respectively, and $\theta_{\mathrm{LO}}(t)$ are the phase of local oscillator. These photo currents $I_{\mathrm{I}}(t)$ and I_{Q} (t) correspond to the I and Q components of the Y-00 signal, respectively. The complex amplitude of the received signal $I_{\mathrm{r}}(t)$ is reconstructed from the eq. (3) and (4) as

$$I_{\mathrm{r}}(t) = R\sqrt{P_{\mathrm{s}}(t)P_{\mathrm{LO}}}\exp\left\{j\left(\theta_{\mathrm{data}}(t)+\theta_{\mathrm{basis}}(t)+\theta_{\mathrm{noise}}(t)\right)\right\} \tag{5}$$

$$\theta_{\mathrm{noise}}(t) = \theta_{\mathrm{sn}}(t)-\theta_{\mathrm{LO}}(t) \tag{6}$$

where $\theta_{\mathrm{noise}}(t)$ is the total phase noise. For stable coherent detection, the phase noise $\theta_{\mathrm{noise}}(t)$, which varies in time, should always be zero. In the following of this section, we focus on symbol-by-symbol estimation of the phase noise $\theta_{\mathrm{noise}}(t)$ in a digital domain. By substituting the estimated phase noise from the reconstructed complex amplitude $I_{\mathrm{r}}(t)$, phase of the data is demodulated.

In the CPE process, a legitimate receiver has pre-shared keys, and the basis selection of each symbol is known, while an eavesdropper cannot use the information. We propose a feedforward CPE that incorporates decryption of Y-00 signal. Fig. 3 shows the block diagram. First, for the decryption, the complex amplitude of signal is multiplied by the exponential function of the opposite phase of the basis.

$$I_{\mathrm{decry}}(i) = I_r(i)\cdot\exp\left(-j\theta_{\mathrm{basis}}(i)\right) \tag{7}$$

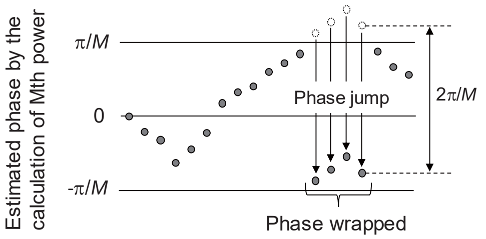

Fig. 4. Phase wrapping in feedforward CPE.

Here the time t is replaced with the identification number of symbol i. The replacement is achieved by retiming the received signal. Then, the phase noise of the decrypted signal $I_{\mathrm{decry}}(i)$ is estimated. An Mth power of the signal complex amplitude is calculated for M-array PSK data modulation, resulting in the cancel of the data modulation ($M\theta_{\mathrm{data}}(i) = 2\pi m$). We figure out a sum of them over $2n+1$ symbols around a symbol to be estimated. This summation process acts as averaging and improves the signal-to-noise ratio (SNR). Then, argument of the summed complex amplitude is divided by M, and the phase noise $\theta_{\mathrm{noise}}(i)$ is estimated as follows.

$$\theta_{\mathrm{est}}(i) = \overline{\theta_{\mathrm{noise}}(i)} = \arg\left[\sum_{l=-n}^{n}\left\{I_{\mathrm{decry}}(i+l)\right\}^M\right]/M \tag{8}$$

We subtract the estimated phase noise from the argument of the signal complex amplitude after the decryption, and obtain a decoded phase of a symbol. This procedure is repeated for every symbols. As shown in Fig. 4, the estimated phase noise is wrapped between $-\pi/M$ to π/M in the CPE. When the absolute value of the estimated phase noise exceeds π/M, phase jump occurs. To avoid the phase jump, phase unwrapping process is implemented. We calculate the difference of the estimated phases between the symbols of i and i-1 as $f(i) = \theta_{\mathrm{est}}(i) - \theta_{\mathrm{est}}(i-1)$. According to the result, the estimated phase is corrected as follows.

$$\theta_{\mathrm{est}}(i) \rightarrow \begin{cases} \theta_{\mathrm{est}}(i)+2\pi/M & (f(i)<-\pi/M) \\ \theta_{\mathrm{est}}(i) & (|f(i)|\le\pi/M) \\ \theta_{\mathrm{est}}(i)-2\pi/M & (f(i)>\pi/M) \end{cases} \tag{9}$$

This correction is based on an assumption that change of the phase noise is contiguous. The amount of the phase change between the adjacent symbols must be less than π/M. For small M, e.g. M = 2, 4, 8, this assumption is valid by a wide margin.

III. Numerical Simulations

We demonstrated digital-coherent detection using the feedforward CPE with Y-00 decryption process in numerical simulations. 10-Gbaud Y-00 signal based on binary PSK was prepared under the condition summarized in Table 1. Phase noises of the signal and local oscillator are mainly caused in a laser. The noise of the laser accumulated during the symbol interval T = 1 / (baud rate) is assumed to follow Gaussian distribution. The variance is $\sigma^2 = 2\pi\delta f T$[16], where δf indicates 3-dB linewidth of the laser. Assuming multi-span transmission with optical amplifiers, white Gaussian noise is added to Y-00 signal.

TABLE I
DETAIL OF PSK Y-00 SIGNAL FOR NUMERICAL SIMULATIONS

Item	Value
Baud rate	10 Gbaud
Data pattern	PRBS 2^{15}-1
Wavelength	1550 nm
Laser linewidth	100 kHz
Number of Y-00 bases	$2^{12} = 4096$

Digital-coherent detection of the signal is realized with the procedure detailed in Sec. II. Since the data modulation is binary PSK, M is set at 2. We check performances of the feedforward CPE with decryption process. Bit error ratio (BER) of Y-00 signal is evaluated for various SNRs. Fig. 5 shows the results when we turn the summation process for averaging off ($n = 0$) or on ($n = 20$). As a reference, BER of binary PSK signal demodulated with a conventional feedforward CPE without the decryption process is plotted. The summation process is effective, resulting in the successful phase tracking. The BER characteristics are comparable between the Y-00 and binary PSK signals. The feedforward CPE with decryption process achieves penalty-less performances.

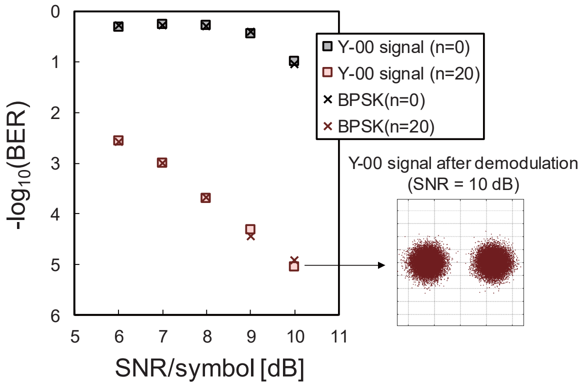

Fig. 5. BER characteristics of PSK Y-00 and binary PSK signals at 10 Gbaud.

IV. DISCUSSION

We discuss digital-coherent detection of Y-00 signal using a conventional feedforward CPE without decryption process. When the decryption process is not implemented, an eavesdropper who has no shared keys can try to use the detection. There are two approaches: one is to use the conventional feedforward CPE ($M = 2$) for estimating sum of the phases of basis modulation and noise. The other is to use the feedforward CPE at a unique setting of very large M for directly obtaining phase noise by canceling both data and basis modulations. The former approach fails, as discussed in [13], Here, we discuss the latter one.

PSK Y-00 signal is considered to be $2N_{\mathrm{basis}}$-array PSK signal when the data modulation is binary. Hence, when M is set at $2N_{\mathrm{basis}}$ in the feedforward CPE, both data and basis modulations are canceled according to the relation of $M(\theta_{\mathrm{data}}(i)+ \theta_{\mathrm{basis}}(i)) = 2\pi m$. For instance, $M = 8192$ for $N_{\mathrm{basis}} = 4096$ in the numerical simulations. However, this CPE does not work properly. The failure is caused by the process of phase unwrapping. As mentioned in Sec. II, the phase unwrapping is based on the assumption that the amount of the phase change between the adjacent symbols is below π/M. This condition becomes tight for large M: if phase noise of a laser exceeds π/M, the phase unwrapping process does not work. We estimate the relation between the phase noise of a laser and π/M. Fig. 6 shows the comparison for various laser linewidths from 1 to 1000 kHz. Three standard deviation of the laser phase noise 3σ is calculated. For the comparison, π/M is shown for $N_{\mathrm{basis}} = 128$ and 512. Even if the laser linewidth is 1 kHz, 3σ of the laser phase noise is larger than π/M at $N_{\mathrm{basis}} = 512$. This estimation indicates that the feedforward CPE without decryption process ($M = 2N_{\mathrm{basis}}$) is not effective in practice when the number of bases N_{basis} is larger than 512. This discussion along with our previous one [14] shows that coherent homodyne detection of Y-00 signal, which is often on the premises of discussion about security, cannot be achieved in practice by an eavesdropper who uses the conventional feedforward CPE without decryption process. Note here that a legitimate receiver who has shared keys does not suffer this issue since M can be set at the number of data modulation multiplicity, e.g. 2 for binary PSK, after the digital decryption process.

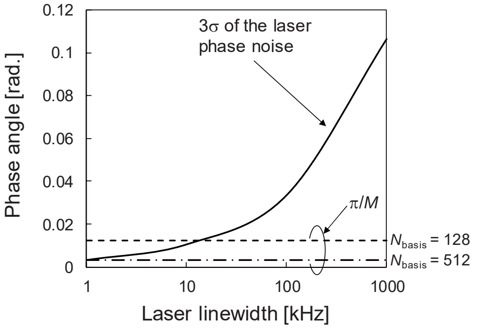

Fig. 6. Comparison between the laser phase noise and π/M.

V. CONCLUSION

We demonstrated digital-coherent detection employing a feedforward CPE with Y-00 decryption process in numerical simulations. In order to estimate phase noise of a laser, an Mth power of complex amplitude was calculated symbol-by-symbol after Y-00 decryption in digital domain. Successful phase tracking of 10-Gbaud PSK Y-00 signal was demonstrated. We also showed that Y-00 signal generated with a large number of bases could not be demodulated with a conventional feedforward CPE without the decryption process.

ACKNOWLEDGMENT

The authors thank K. Kato for fruitful discussions.

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, "Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol," Phys. Rev. A, 76, 032307, 2007.

[3] 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.

[4] 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," in Proc. OECC, MO1A2, 2014.

[5] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen "Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks," Phys. Rev. A 71(6), 062326, 2005.

[6] C. Liang, G. S. Kanter, E. Corndorf, and P. Kumar, "Quantum Noise Protected Data Encryption in a WDM Network," IEEE Photon. Technol. Lett, vol. 17, no. 7, pp. 1573-1575, 2005.

[7] 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.

[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] 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.

[10] 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.

[11] K. Kato, "A unified analysis of optical signal modulation formats for quantum enigma cipher," Proc. SPIE 10409, Quantum Communications and Quantum Imaging XV, 104090K, 2017.

[12] D.-S. Ly-Gagnon, S. Tsukamoto, K. Katoh, and K. Kikuchi, "Coherent detection of optical quadrature phase-shift keying signals with carrier phase estimation," J. of Lightwave Technol., vol.24, no.1, pp.12- 21, 2006.

[13] S. Tsukamoto, K. Katoh, and K. Kikuchi, "Unrepeated transmission of 20-Gbit/s optical quadrature phase-shift keying signal over 200-km standard single-mode fiber based on digital processing of homodyne-detected signal for group-velocity dispersion compensation," IEEE Photon. Technol. Lett., vol.18, no.9, pp.1016-1018, 2006.

[14] K. Tanizawa, F. Futami, and O. Hirota, " Digital feedforward carrier phase estimation for PSK Y-00 quantum-noise randomized stream cipher," IEICE Communications Express, submitted.

[15] T. G. Hodgkinson, R. A. Harmon, and D. W. Smith, "Demodulation of optical DPSK using in-phase and quadrature detection," Electron. Lett., vol. 21, pp. 867-868, 1985.

[16] K. Kikuchi, T. Okoshi, M. Nagamatsu, and N. Henmi, "Degradation of bit-error rate in coherent optical communications due to spectral spread of the transmitter and the local oscillator," J. of Lightwave Technol., vol. LT-2, no. 6, pp. 1024–1033, 1984.