Digital feedforward carrier phase estimation for PSK Y-00 quantum-noise randomized stream cipher

Ken Tanizawa\textsuperscript{a)}, Fumio Futami, and Osamu Hirota

Quantum ICT Research Institute, Tamagawa University,
6–1–1 Tamagawagakuen, Machida, Tokyo 194–8610, Japan

\textsuperscript{a)} tanizawa@lab.tamagawa.ac.jp

Abstract: Encryption in fiber-optic transmission is one of remaining issues in modern communication systems. One of the solutions is to use Y-00 quantum-noise randomized stream cipher. In this paper, we propose feedforward carrier phase estimation (CPE) with Y-00 decryption process for digital-coherent detection of phase-shift keying (PSK) Y-00 signal. After decryption of Y-00 signal in a digital domain, carrier phase is estimated by calculating Mth power of signal complex amplitude. Numerical simulations for 10-Gbaud PSK Y-00 signal show that the feedforward CPE with decryption process, which is used by a legitimate receiver who shares keys, successfully tracks phase noise. Consequently, penalty-less demodulation of Y-00 signal is achieved.

Keywords: secure communications, digital coherent transmission

Classification: Fiber-Optic Transmission for Communications

References

[1] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure communication using mesoscopic coherent states,” \textit{Phys. Rev. Lett.}, vol. 90, no. 22, p. 227901, 2003. DOI:10.1103/PhysRevLett.90.227901

[2] 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,” \textit{Phys. Rev. A}, vol. 71, no. 6, p. 062326, 2005. DOI:10.1103/PhysRevA.71.062326

[3] O. Hirota, M. Sohma, M. Fuse, and K. Kato, “Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme,” \textit{Phys. Rev. A}, vol. 72, no. 2, p. 022335, 2005. DOI:10.1103/PhysRevA.72.022335

[4] K. Kato and O. Hirota, “Quantum quadrature amplitude modulation system and its applicability to coherent state quantum cryptography,” \textit{Proc. SPIE}, vol. 5893, p. 589303, 2005. DOI:10.1117/12618719

[5] M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai, “QAM quantum stream cipher using digital coherent optical transmission,” \textit{Opt. Express}, vol. 22, no. 4, pp. 4098–4107, 2014. DOI:10.1364/OE.22.040908

[6] C. Liang, G. S. Kanter, E. Corndorf, and P. Kumar, “Quantum noise protected data encryption in a WDM network,” \textit{IEEE Photonics Technol. Lett.}, vol. 17, no. 7, pp. 1573–1575, 2005. DOI:10.1109/LPT.2005.848264
1 Introduction

Encryption of data in transmission system is important, because transmission system faces a potential threat of eavesdropping. Not only high layers but also the lowest physical layer or fiber-optic transmission should be protected from such a threat. An approach for secure fiber-optic transmission is to use a physical cipher technology. Particularly, Y-00 quantum-noise randomized stream cipher [1], which is a symmetric-key direct data encryption scheme that utilizes masking by quantum noise, is promising in terms of compatibility with modern fiber-optic networks where vast amount of data is transmitted in a high data rate of more than Gbit/s. Y-00 signal (ciphertext in Y-00 encryption scheme) is generated based on multi-level modulation of phase [1, 2], intensity [3], or quadrature amplitudes [4, 5].

We focus on the phase modulation in this paper. So far, in the experimental demonstrations of phase-shift-keying (PSK) Y-00 signal transmission [2, 6], decryption was realized in an optical domain with a phase modulator, and differential detection using a 1-bit delay interferometer was employed. On the other hand, the recent progress of digital-coherent detection is tremendous [7]. Carrier phase estimation (CPE) which tracks phase noise of received signal for homodyne detection [8] and compensation of linear distortion caused by transmission over optical fibers [9] are achieved stably in a digital domain, which enables long reach transmission at a high data rate. It is important to clarify the effectiveness of such a powerful digital-coherent detection in PSK Y-00 signal transmission.

As a first step, this paper reports on digital feedforward CPE for PSK Y-00 signal. Decryption of Y-00 signal in a digital domain is incorporated with a feedforward CPE which cancels out data modulation by calculating an M-th power of a complex amplitude of received signal. We demonstrate digital-coherent detection using the feedforward CPE with Y-00 decryption process in numerical
simulations. Successful tracking of phase noise and penalty-less demodulation are achieved for 10-Gbaud PSK Y-00 signal.

2 Digital feedforward CPE for PSK Y-00 signal

PSK Y-00 encryption utilizes multi-level phase modulation. Fig. 1(a) shows the mapping of Y-00 signal based on binary PSK data modulation in an I-Q plane. The signal phase is modulated to 0 or \( \pi \) by binary data. At the same time, the basis (communication basis) of the phase modulation \( \theta_{\text{basis}} \) is selected randomly between 0 to \( \pi \) in a symbol-by-symbol manner. The random basis selection is given using a mathematical encryption box with a key shared between legitimate users. The complex amplitude of the Y-00 signal \( I_{Y00}(t) \) is expressed as

\[
I_{Y00}(t) = A_s(t) \exp\{j(\theta_{\text{data}}(t) + \theta_{\text{basis}}(t))\}
\]

where \( A_s(t) \) is amplitude, and \( \theta_{\text{data}}(t) \) and \( \theta_{\text{basis}}(t) \) are the phases of the data and basis modulations, respectively. The basis should be modulated in a high resolution; that is, the number of bases \( N \) should be large. Then, the distance between adjacent bases, \( \Delta \theta_{\text{basis}} = |\theta_{\text{basis},x} - \theta_{\text{basis},x-1}| \), is very short. For strong randomization of the basis selection, the distance should be much less than the standard deviation of quantum noise.

Coherent detection of Y-00 signal is realized with a phase-diversity homodyne coherent receiver that consists of a local laser, a 90-degree optical hybrid circuit and two balance photo detectors [10]. Then, the complex amplitude of the received signal \( I_r(t) \) is reconstructed as

\[
I_r(t) = R \sqrt{P_s(t)P_{LO}} \exp\{j(\theta_{\text{data}}(t) + \theta_{\text{basis}}(t) + \theta_{\text{noise}}(t))\}
\]

where \( R \) is the responsivity of a photodiode, \( P_s(t) \) and \( P_{LO} \) are the powers of the signal and local oscillator, respectively, and \( \theta_{\text{noise}}(t) \) is the phase noise which varies

![Fig. 1. (a) Signal constellation, and (b) feedforward carrier phase estimation of PSK Y-00 signal.](image-url)
We focus on the estimation of the phase noise $\theta_{\text{noise}}(t)$ in a digital domain after the detection. In the CPE process, a legitimate receiver has a pre-shared key, and the basis selection of each received symbol is known.

We incorporate decryption process of Y-00 signal into a feedforward CPE that calculates an $M$-th power of a signal complex amplitude for $M$-ary PSK. Fig. 1(b) shows the block diagram. A block for the decryption is added before the feedforward CPE. The complex amplitude of the signal is multiplied by the exponential function of the opposite phase of the basis. Then, the phase noise of the decrypted signal is estimated. An $M$-th power of the signal complex amplitude is calculated for each symbol to strip the data modulation. We figure out a sum of them over $2n + 1$ symbols around a symbol to be estimated for improving the signal-to-noise ratio (SNR). Next, argument of the summed complex amplitude is calculated. The phase is divided by $M$, and the phase noise $\theta_{\text{noise}}(i)$ is estimated as

$$\theta_{\text{est}}(i) = \frac{\theta_{\text{noise}}(i)}{M} = \frac{\arg\left[\sum_{l=-n}^{n} \{I_r(i + l) \cdot \exp(-j\theta_{\text{basis}}(i + l))\}^M\right]}{M}$$

where the time $t$ is replaced with the identification number of symbol $i$. The replacement is achieved by retiming the received signal. 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. The estimated phase noise is wrapped between $-\pi/M$ to $\pi/M$ in the feedforward CPE, and phase jump occurs when the absolute value of the estimated phase noise exceeds $\pi/M$. To avoid it, phase unwrapping that corrects such phase jumps is implemented. The phase unwrapping is based on an assumption that a change rate of the phase noise is slower than a symbol rate.

### 3 Numerical simulations

We conducted numerical simulations of digital-coherent detection using the feedforward CPE with decryption process. 10-Gbaud Y-00 signal based on binary PSK was generated in the following conditions: the data pattern was pseudo-random bit sequence (PRBS) of $2^{15} - 1$, and the number of Y-00 bases $N$ was $2^{12} = 4096$. A linewidth of lasers for the transmitter and local oscillator $\delta f$ was $100$ kHz. Phase noise of the laser accumulated during the symbol interval $T = 1/(\text{baud rate})$ is assumed to follow Gaussian distribution with a variance of $\sigma^2 = 2\pi\delta f T$ [11]. To simulate multi-span transmission with optical amplifiers, white Gaussian noise is added.

We checked performances of the feedforward CPE with decryption process when the SNR per symbol was $15$ dB. Since the data modulation was binary PSK, $M$ was set at $2$. The number of symbols for the summation process $n$ was set to $10$. Fig. 2(a) shows the constellation diagrams of Y-00 signal and signal after demodulation with the feedforward CPE. Demodulation is successfully achieved. Bit errors are not observed in this SNR. Fig. 2(b) shows tracking of the phase noise. The feedforward CPE successfully tracks accumulated phase noise.

Next, we evaluate bit error ratio (BER) of Y-00 signal after demodulation for various SNRs. Two CPE methods are considered: one is the feedforward CPE with
decryption process, which can be used by a legitimate user; and the other is a
conventional feedforward CPE \((M = 2, \text{ and } n = 10)\) without decryption process.
Fig. 3 shows the results. For a reference, BER of binary PSK signal demodulated
with the conventional feedforward CPE is plotted. The BER characteristics are
comparable between the Y-00 signal demodulated by the feedforward CPE with
decryption process and the binary PSK signal. Penalty-less demodulation of the
Y-00 signal is achieved. On the other hand, the BER of Y-00 signal demodulated
with the conventional feedforward CPE is approximately 0.5 regardless of SNR.
The reason is discussed in the next section.

![Fig. 2. Performances of the feedforward CPE with Y-00 decryption process: (a) Constellation diagrams and (b) tracking of phase noise.](image)

![Fig. 3. BER characteristics of Y-00 signals demodulated by the feedforward CPE with and w/o Y-00 decryption process.](image)

### 4 Discussion

Here we discuss the reason why the conventional feedforward CPE in which \(M\) is
set at the number of multilevels of data modulation \((M = 2 \text{ in the simulation})\) does
not work for Y-00 signal properly. When an \(M\)-th power of a received complex
amplitude is calculated, the PSK data modulation is stripped, and \(M(\theta_{basis}(i) +\)
\( \theta_{\text{noise}}(i) \) is obtained. After divided by \( M \), a sum of the phases of the basis and noise, \( \theta_{\text{est}}(i) = \theta_{\text{basis}}(i) + \theta_{\text{noise}}(i) \), is likely to be estimated. One may think that the decryption process added before the phase estimation is not necessary. However, the simulation results did not support it. As mentioned in Sec. 2, the \( M \)-th powers of signal complex amplitudes are summed up for improving SNR of the estimation. This process causes a significant negative impact. Due to the symbol-by-symbol basis selection, \( \theta_{\text{basis}}(i) \) is not constant within the summation period (\( n = 10 \) in the simulation), while \( \theta_{\text{noise}}(i) \) is almost constant. Hence, the phase of the basis for a certain symbol can never be estimated from the summed or averaged value.

Next, let us think when we give up the summation, or \( n = 0 \). This sacrifices SNR of the estimation, and the feedforward CPE cannot work properly in a low SNR range. Even so, it is meaningful to consider a case of ultimately high SNR, which is limited only by the shot noise. In the case, the conventional feedforward CPE failed, and BER was approximately 0.5 in the simulation. This can be explained as follows. The feedforward CPE employs the phase unwrapping, where \( 2\pi/M \) is summed or subtracted from the estimated phase \( \theta_{\text{est}}(i) \) when \( |\theta_{\text{est}}(i) - \theta_{\text{est}}(i-1)| > \pi/M \) (\( M = 2 \) in our case). For Y-00 signal, the condition of \( |\theta_{\text{est}}(i) - \theta_{\text{est}}(i-1)| > \pi/2 \) is randomly satisfied with a probability of 0.5 since the phase of the basis is modulated randomly between \( 0 \) to \( \pi \) in a symbol-by-symbol manner. This induces incorrect phase unwrapping, resulting in the BER of 0.5. In other words, the phase unwrapping is effective when the estimated phase is contiguous.

## 5 Conclusion

We proposed a feedforward CPE for PSK Y-00 quantum-noise randomized stream cipher signal. An \( M \)-th power of received complex amplitude was calculated for stripping the data modulation after Y-00 decryption process in a digital domain. Successful phase tracking of 10-Gbaud PSK Y-00 signal was numerically demonstrated. We also showed that Y-00 signal could not be demodulated properly when the conventional feedforward CPE without decryption process (\( M = 2 \)) was employed.

**Acknowledgments**

The authors thank K. Kato for fruitful discussion.