ISSN 2186-6570

Practical Design Consideration of PSK Y-00 Quantum Stream Cipher Based on *M*-ary Data Modulation

Ken Tanizawa and Fumio Futami

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

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.9, No.1, 49-52, 2019

Practical Design Consideration of PSK Y-00 Quantum Stream Cipher Based on *M*-ary Data Modulation

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

***Abstract*—This paper reports security analysis of phase-shift keying (PSK) Y-00 quantum stream cipher and a design approach of the cipher system in consideration of the security. A primal measure of the security of Y-00 cipher is a quantum-noise masking number which indicates the number of signal levels masked by shot noise. We define the masking number for PSK Y-00 cipher based on *M*-ary data modulation and discuss the probability that an eavesdropper without a seed key correctly discriminates cipher symbols. Practical design parameters of the cipher with which we achieve a very low probability of the correct discrimination can be fixed in this approach.**

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

I. Introduction

In fiber-optic transmission, signal interception or tapping from installed fiber cables is a potential security risk. To introduce cipher in the physical layer is effective for direct protection of tapping. Since current optical transmission systems achieve high capacity and a long reach, cipher systems need to be compatible with such features for practical uses. A promising approach is symmetric-key direct data encryption based on secrecy realized by signal masking due to quantum (shot) noise [1]. The quantum-noise masking is achieved with an extremely high-order optical modulation using a pre-shared seed key. After the modulation for encryption, the distance between adjacent optical signals reduces extremely, and discrimination of the signal is inherently prevented by the effect of shot noise. Such cipher systems were demonstrated as AlphaEta [2] or Y-00 quantum stream cipher [3]. Masking by shot noise promises irreducible and unchanged security because shot noise is inherently inevitable and truly random. Moreover, this cipher system is compatible with current dense WDM systems using optical amplifiers [4].

Here, Y-00 cipher based on phase-shift keying (PSK) modulation, where an *M*-ary PSK data signal is encrypted only by random phase rotation, is focused on. In the early stage of the research, 622-Mbit/s (OC-12) and 2.66-Gbit/s (OC-48) cipher systems based on binary data modulation ($M = 2$) were demonstrated as AlphaEta [5], [6]. Recently, we have introduced digital coherent technology to the cipher for higher capacity. A 10-Gbit/s digital coherent PSK Y-00 cipher system was achieved with two key enabling techniques: coarse-to-fine phase randomization for the encryption and digital decryption incorporated into digital signal processing (DSP) for intradyne coherent detection were proposed and demonstrated [7]. Moreover, in order to increase the bit rate, we employed polarization multiplexing and higher-order data modulation ($M = 4$) and achieved 48-Gbit/s PSK Y-00 cipher transmission [8].

One of security measures in Y-00 cipher is a quantum-noise masking number that indicates the number of signal levels masked by shot noise. In our previous work [9], tradeoffs between the masking number and transmission reach were theoretically analyzed. It was confirmed that the tradeoff was independent of a baud rate of the cipher. The tradeoff relation indicated that masking number of more than 100 was achievable for long-reach transmissions. While the quantum-noise masking number is a primal measure of security, further security assessment is meaningful for practical uses. In this paper, we report theoretical analysis of the probability that an eavesdropper without the seed key discriminates correct phase levels of the cipher. Such security assessment for PSK Y-00 cipher based on binary data modulation was partially provided in [10]. Here, the analysis is extended to PSK Y-00 cipher based on *M*-ary data modulations. First, the masking number for PSK Y-00 cipher based on *M*-ary data is derived. Then, relation between the probability of correct discrimination and masking number is obtained. Using these two relations, we can fix design parameters of the cipher, e.g. the optical average power and bit number of bases, for a target low probability.

II. Signal Making Due To Quantum (Shot) Noise

Extremely high-order phase modulation is employed for the encryption in PSK Y-00 cipher. Fig. 1 shows the operating principle of PSK Y-00 cipher based on QPSK data modulation ($M = 4$). The left diagram shows the constellation of QPSK data modulation before encryption, in which a symbol is mapped to $\pi/4$, $3\pi/4$, $5\pi/4$, or $7\pi/4$ in an I/Q plane. The arrow on I axis indicates the basis of the phase modulation. For the encryption, 2^m bases are prepared and one of them is selected in a symbol-by-symbol manner. The basis is determined randomly utilizing a seed key that is pre-shared between legitimate users. The right diagram shows the constellation of PSK Y-00 cipher. The bit resolution m is set to a large number, e.g., 10 or more. Then, the constellation of Y-00 cipher becomes extremely high-order PSK which has $M{\cdot}2^m$ phase levels in total.

Here, we discuss signal masking due to the shot noise in the PSK Y-00 cipher. Fig. 2 shows the magnified image of the

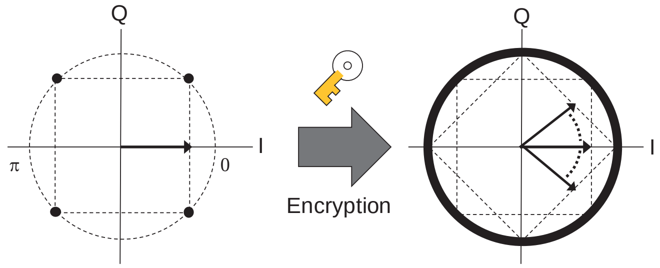


Fig. 1. Symbol mapping of PSK Y-00 cipher based on QPSK data.

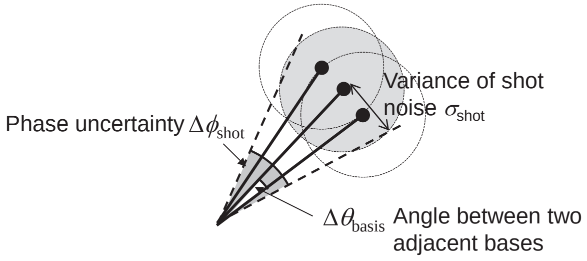

Variance of shot noise σ_{shot}
Phase uncertainty $\Delta\phi_{\text{shot}}$
$\Delta\theta_{\text{basis}}$ Angle between two adjacent bases

Fig. 2. Magnified image of the symbols in PSK Y-00 cipher.

cipher. The phase uncertainty caused by shot noise $\Delta\phi_{\text{shot}}$ is expressed as

$$\Delta\phi_{\text{shot}} = \frac{\frac{1}{2}}{\sqrt{n}} \tag{1}$$

where n is the average number of photons of a symbol. When the data is modulated at a baud rate of R, n is obtained as

$$n = \frac{P_0}{R \cdot h\nu_0} \tag{2}$$

where P_0, h, and ν_0 are the signal average power, Planck constant, and signal frequency, respectively. When M-ary PSK data modulation is employed, the angle between adjacent bases shown in Fig. 2, $\Delta\theta_{\text{basis}}$, is calculated as

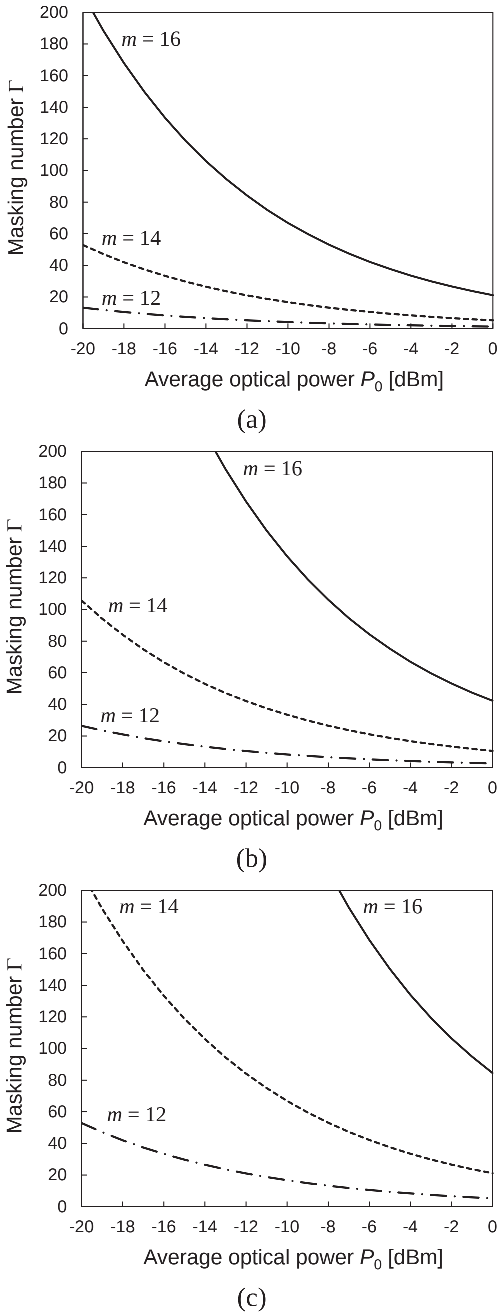
$$\Delta\theta_{\text{basis}} = \frac{2\pi}{M \cdot 2^m} \tag{3}$$

where M and m indicate the order of data modulation and the bit number of bases, respectively. Here, a quantum-noise masking number Γ, which indicates the number of signal phase levels covered by the variance of the shot noise, is introduced as a security measure of PSK Y-00 cipher. The masking number is calculated as follows.

$$\Gamma = \frac{\Delta\phi_{\text{shot}}}{\Delta\theta_{\text{basis}}} = \frac{M \cdot 2^m}{4\pi}\sqrt{\frac{R \cdot h\nu_0}{P_0}} \tag{4}$$

A higher masking number is better for security. The masking number is related to the signal parameters such as M, R, ν_0, and P_0. Also, the number is proportional to the number of bases 2^m.

Next, we investigate the quantum-noise masking number Γ when the average optical power P_0 and the bit number of bases m are changed. The signal baud rate R and frequency ν_0 are set to 32 Gbaud and 1550 nm, respectively. Fig. 3 shows the results when the data modulations are (a) BPSK (M=2), (b) QPSK (M=4), and (c) 8 PSK (M=8). These results are guidelines to determine the parameters of PSK Y-00 cipher in practice. For example, when the data modulation is QPSK and the encryption is performed with m of 16, optical power should be less than approximately -8 dBm for a masking number higher than 100. The optical power at the output of a transmitter is highly related to the reach of transmission. The relation between the reach and masking number was discussed in our previous work [9]. Note also here that direct comparison among Figs. 3(a)-(c) is not meaningful because of the following two reasons. These curves are plotted under the condition of the same baud rate, and hence the bit rates are different. Moreover, in general, average optical power required to achieve the same signal quality after the transmission over the same distance is different among the order of data modulation M.



(a)

(b)

(c)

Fig. 3. Quantum-noise masking numbers of 32-Gbaud PSK Y-00 cipher based on the data modulation of (a) BPSK, (b) QPSK, and (c) 8 PSK.

III. Discrimination of Cipher Symbols without Key

The quantum noise masking number is a primal measure of security in PSK Y-00 cipher. Here, practical security is discussed based on the masking number. A typical procedure to attack on a seed key is as follows: an eavesdropper intercepts the cipher which has $M\cdot 2^m$ phase levels, and then the cipher is analyzed with computational power. Since the subsequent analysis is effective for correctly measured symbols of the cipher, the discrimination of phase levels is important as the first step. The probability that an eavesdropper without a seed key correctly measures one symbol of the cipher $P_{\mathrm{eve\_symbol}}$ is calculated based on the model of multilevel signal detection, as shown in Fig. 4.

$$P_{\mathrm{eve\_symbol}} = \int_{A_i-\frac{\Delta_{\mathrm{basis}}}{2}}^{A_i+\frac{\Delta_{\mathrm{basis}}}{2}} \frac{1}{\sqrt{2\pi\sigma_{\mathrm{shot}}{}^2}} exp\left(-\frac{(x-A_i)^2}{2\sigma_{shot}{}^2}\right) dx$$

$$= erf\left(\frac{\frac{\Delta_{\mathrm{basis}}}{2}}{\sqrt{2}\sigma_{\mathrm{shot}}}\right) \qquad (5)$$

Here, since the number of photons are large, it is assumed that shot noise has Gaussian distribution with a standard deviation of σ_{shot}. A_i and Δ_{basis} indicate the phase value of i-th signal of the cipher and the phase distance between adjacent signals, respectively, as shown in Fig. 4. When the number of phase levels is large, the angle between adjacent bases $\Delta\theta_{\mathrm{basis}}$ and the angle of the variance of shot noise $\Delta\phi_{\mathrm{shot}}$, which are defined in Fig. 2, are small. Then, the masking number Γ is approximated as follows.

$$\Gamma = \frac{2\sigma_{\mathrm{shot}}}{\Delta_{\mathrm{basis}}} \qquad (6)$$

By substituting eq. (6) into Eq. (5), the probability $P_{\mathrm{eve\_symbol}}$ can be expressed as a function of the masking number Γ.

$$P_{\mathrm{eve\_symbol}} = erf\left(\frac{1}{\sqrt{2}\Gamma}\right) \qquad (7)$$

It can be seen that the masking number is related directly to the security against the typical attack where the eavesdropper tries to correctly measure the cipher.

In practice, success of the discrimination of one symbol is not enough to deduce the seed key. Provided that the length of consecutive symbols l is required to deduce the seed key, the probability $P_{\mathrm{eve\_key}}$ is obtained as follows.

$$P_{\mathrm{eve\_key}} = \left[erf\left(\frac{1}{\sqrt{2}\Gamma}\right)\right]^l \qquad (8)$$

The symbol length l is related to the length of the seed key and the complexity of pseudorandom number generator (PRNG) which is used to extend the seed key to key stream. Fig. 5 shows $P_{\mathrm{eve\_key}}$ for various masking numbers at l of 16, 32, and 64. Higher masking number and longer l are necessary for high security of the system. The design parameters of PSK Y-00 cipher are the bit number of bases m, optical average power P_0, the length of a seed key, and complexity of PRNG. Using Fig. 3 and Fig. 5, we can set these parameters for a target $P_{\mathrm{eve\_key}}$. A design for a target $P_{\mathrm{eve\_key}}$ of 10^{-70}, provided that the baud rate is 32 Gbaud and that the data modulation is QPSK, is determined as follows. The masking number of 123 is necessary to achieve the target probability when l is 32. Then, optical power at the output of the transmitter is set to be -9.3 dBm, provided that m is 16. Thus, we can fix the design parameters in PSK Y-00 cipher systems.

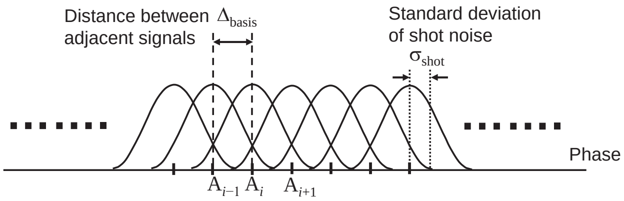

Distance between adjacent signals
Δ_{basis}
Standard deviation of shot noise
σ_{shot}
Phase
A_{i-1}
A_i
A_{i+1}

Fig. 4. A model of multi-level phase detection.

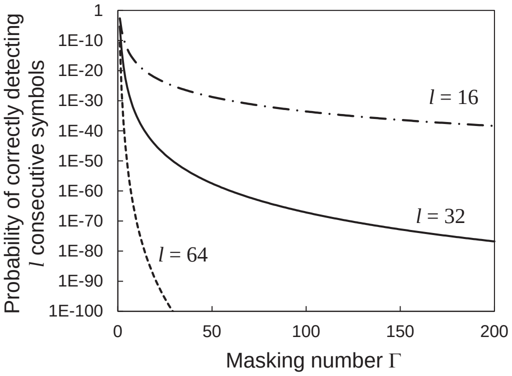


Fig. 5. Probability of discriminating consecutive l symbols of the cipher for various masking numbers.

IV. Conclusion

We have reported practical design approach in consideration of the security for PSK Y-00 quantum stream cipher based on M-ary data modulation. The quantum-noise masking number, which is defined as the number of phase levels covered by shot noise, is defined as a function of design parameters such as the order of data modulation, bit number of bases, baud rate, frequency, and optical average power. Then, the relation between the masking number and the probability that an eavesdropper without a seed key correctly discriminates symbols of the cipher is derived. Using the relations, we can determine the design parameters of PSK Y-00 cipher with which a very low probability of the discrimination or high security is promised.

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] 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.

[3] 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.

[4] F. Futami, K. Guan, J. Gripp, K. Kato, K. Tanizawa, C. Sethumadhavan, and P. J. Winzer, “Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system,” Optics Express, vol. 25, no. 26, pp. 33338-33349, 2017.

[5] 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.

[6] G. S. Kanter, S. X. Wang, R. A. Lipa, and D. Reilly, "Self-Coherent Differential Phase Detection for Optical Physical-Layer Secure Communications," in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2013, OSA Technical Digest (online) (Optical Society of America, 2013), paper JW2A.41.

[7] K. Tanizawa and F. Futami, "Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels," Opt. Express vol. 27, pp. 1071-1079, 2019.

[8] K. Tanizawa and F. Futami, "Single channel 48-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF," Opt. Express vol. 27, pp. 25357-25363, 2019.

[9] K. Tanizawa, and F. Futami, "Trade-offs Between Masking Number and Transmission Reach in Digital-Coherent PSK Y-00 Quantum Stream Cipher, " Tamagawa University Quantum ICT Research Institute Bulletin, vol. 8, no. 1, pp. 9-12, 2018.

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