ISSN 2186-6570

Theoretical Investigation of Noise Masking Effect by Quantum Noise in Intensity Modulation Y-00 Quantum Stream Cipher

Fumio Futami, and Ken Tanizawa

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, 45-47, 2019

Theoretical Investigation of Noise Masking Effect by Quantum Noise in Intensity Modulation Y-00 Quantum Stream Cipher

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

***Abstract*— A Y-00 quantum stream cipher employs noise masking to protect the interception of ciphertext. Among several kinds of noise, quantum noise, or shot noise, is inevitable during detection. Therefore, an investigation of noise masking using quantum noise is beneficial, although much larger noises, such as amplified spontaneous emission noise, are dominant in actual optical fiber communication systems. In this work, we first derive an analytical solution for quantum noise masking. Next, a probability of correct guessing of ciphertext is analyzed under some assumptions and is numerically calculated. The probability of correct guessing of the Y-00 cipher transceiver fabricated by us was also calculated.**

***Index Terms* — Y-00 quantum stream cipher, physical cipher, noise masking, correct guessing, ciphertext, secure optical communication.**

I. Introduction

Y-00 quantum stream cipher [1-3] is a promising candidate for an optical transport layer with high security to protect eavesdropping, as it features, in addition to high secrecy, high compatibility with deployed optical fiber communication systems such as wavelength-division multiplexed (WDM) systems [4,5], digital-coherent transmission systems [6], and long transmissions [7,8]. A Y-00 cipher realizes secure communication by the combined use of physical randomness and mathematical complexity. The noise masking effect of the physical randomness makes discrimination of a correct cipher signal level difficult. To date, Y-00 cipher security has been theoretically investigated and the general property of a Y-00 cipher has been clarified [9]. We also focused on physical randomness and derived an analytical solution for the probability of correct guessing of ciphertext by an eavesdropper under some assumptions, and numerically calculated the probability achieved by the simplified spontaneous emission (ASE) noise [10]. Among several kinds of noise in a Y-00 cipher, quantum noise, or shot noise, is truly random. Therefore, investigation of the quantum noise masking effect is beneficial from a theoretical viewpoint, although the quantum noise itself is much smaller than ASE noise, and is generally not the limiting factor of the transmission performance of optical fiber communication systems.

In this work, we focus on an investigation of noise masking using shot noise of an intensity modulation (IM) Y-00 cipher, which leads to an analytical solution. In addition, the probability of correct guessing of the ciphertext by an eavesdropper is investigated, and an approximate analytical solution of a probability of correct ciphertext guessing, using noise masking by shot noise, is derived under some assumptions. We calculate the probability numerically for some parameters, including those of the IM Y-00 cipher transceiver that we fabricated [11].

II. Noise masking by shot noise

Here we discuss noise masking produced by quantum noise, where quantum noise means shot noise. First, an equation expressing the amount of shot noise is derived for multi-level intensity modulation signals, as shown in Fig. 1. The number of intensity levels is 2M, where M is the number of bases that are pairs of binary signals “0” and “1”. The maximum and minimum powers are P_{2M} and $P_{1,}$, respectively.

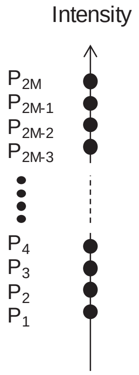

Fig. 1. Multi-level intensity modulation signals where P_{2M} is the highest power and P_1 is the lowest level power.

The number of photons, N_{ph}, in an optical power of P_0 is given by

$$N_{ph} = \frac{P_0}{h\nu_0} \tag{1}$$

where h is the Planck constant and ν_0 is the frequency of the optical signal. Using an ideal photodetector (PD), with a responsivity of 1, for optical-to-electric (OE) conversion, the signal current

$$I_0 = \frac{eP_0}{h\nu_0} \tag{2}$$

is derived where e denotes the elementary charge. When the signal bandwidth is defined to be R, the variance of shot noise current is expressed as

$$\sigma_{shot}^{2} = 2eI_0R \tag{2}$$

and shot noise is represented by

$$\sigma_{shot} = \sqrt{2eI_0R} = e\sqrt{2P_0R/h\nu_0} \tag{3}$$

Shot noise is proportional to the square root of P_0 for a bandwidth of R and frequency of ν_0. The power difference of neighboring signal levels is

$$\Delta\mathrm{P}_{basis} = \frac{P_{2M} - P_1}{2M - 1} \tag{5}$$

Assuming the ideal PD is utilized for OE conversion, the amount of noise masking is defined using shot noise and the minimum power difference as

$$\Gamma_{IM} = \frac{2\sigma_{shot}}{\Delta P_{basis}} = \frac{2(2M-1)e}{P_{2M} - P_1}\sqrt{\frac{2RP_0}{h\nu_0}} \tag{6}$$

The noise masking number of an IM Y-00 cipher is related to such parameters as the number of bases, signal frequency, signal bandwidth and the maximum and minimum signal powers. The maximum power level of P_{2M} has the highest signal power and the minimum power level of P_1 has the lowest. To effectively generate a higher noise masking number for the lower power level signals in an IM Y-00 cipher, a DC offset is intentionally added to the minimum power level signal. Substitution of the ratio of the maximum power to the minimum power, $r = P_{2M} / P_1$ in Eq.(6) leads to

$$\Gamma_{IM} = \frac{(2M-1)(r+1)e}{r-1}\sqrt{\frac{2R}{P_0h\nu_0}} \tag{7}$$

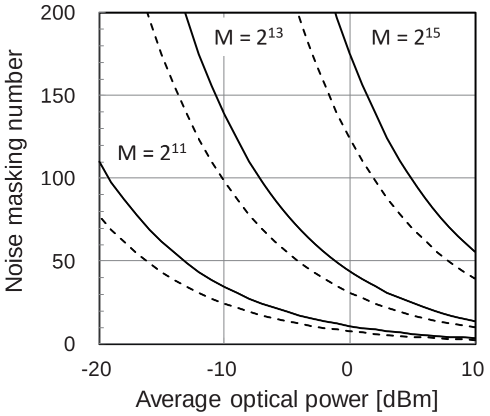

Fig. 2. Dependence of noise masking number of an IM Y-00 cipher on average optical powers and the number of bases.

Using Eq. (7), the noise masking number is calculated when the average signal power and number of bases re changed. In the calculation, the wavelength of the signal is set to λ = 1550 nm which corresponds to ν_0 = c/λ = 193.4 THz. The max-to-min power ratio is set to r = 2. The signal bandwidth is R = 1.5 GHz. Fig.2 shows the noise masking numbers for M = 2^{11}, 2^{13}, and 2^{15} when the average power is changed from -20 dBm to 10 dBm. Solid curves and dashed curves show the numbers for the minimum and maximum powers, respectively. The result indicated that smaller powers and higher number of bases are preferable for realizing high noise masking numbers. The lowest power is determined by the design of the optical fiber communication system where a Y-00 cipher is utilized.

Next, noise masking numbers are calculated when the number of bases and average optical powers are changed, as shown in Fig. 3. One can obtain the required number of bases for the desired number of noise masking by assuming the average optical power, signal bandwidth, and max-to-min ratio.

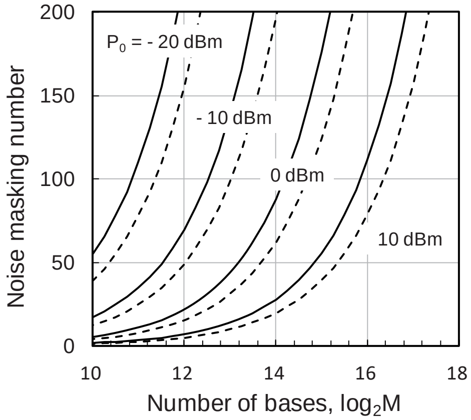

Fig. 3. Dependence of noise masking number of an IM Y-00 cipher on the number of bases and average optical powers.

III. Correct Guessing of Ciphertext by Eavesdropper

Here, we discuss the possibility of correct guessing of ciphertext by an eavesdropper under some assumptions [10]. Here, we assume that an eavesdropper observes a multi-level ciphertext signal and tries estimating the correct power level. As the optical power used for this cipher is generally higher than the order of micro watt, and the quantum noise distribution of the Poisson distribution is shaped like the Gaussian profile for such optical powers, the Gaussian power distribution shown in Fig. 3 is assumed. The Y-00 cipher uses multilevel signals that are placed at the same interval, as shown in Fig. 3.

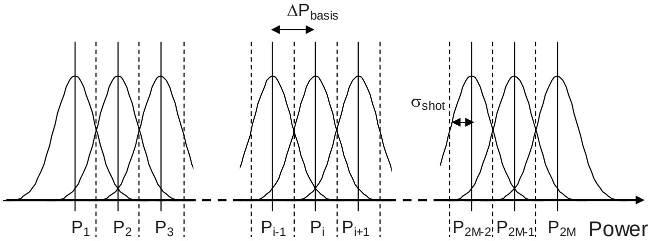

Fig. 4. Model of measurement result by an eavesdropper for multi-level intensity modulation signals.

First, we discuss an eavesdropper's success probability of correct detection of the signals through a simple approximation model. Suppose there are 2M signals and each average of the received signal levels is denoted by P_i, where $1 \le i \le 2M$. Then, the interval is represented by $\Delta P = P_{i+1} - P_i$. (= ΔP_{basis}). Let v denote a measurement outcome for an eavesdropper. In the following analysis, we assumed that direct detection is performed, and the probability distributions of the measurement result can be approximated by Gaussian. Further, to simplify our analysis, we assume that each variance of the distribution is represented by the same value σ_{shot}^2. The probability of correct signal detection at a single time slot is derived under these assumptions as

$$P_{E\_Single} = 1 - \frac{2M-1}{2M} erfc\left[\frac{\Delta P_{basis}}{2\sigma_{shot}\sqrt{2}}\right]$$
$$= 1 - \frac{2M-1}{2M} erfc\left[\frac{1}{\Gamma_{IM}\sqrt{2}}\right] \quad (8)$$

where erfc[·] is the complementary error function. The details of the derivation of this solution is described in [10]. The probability of correct signal detection at a single time slot is expressed by the parameters of the number of bases and the amount of noise masking. Considering the number of bases is high, Eq. (8) is approximately expressed using only Γ_{IM} as

$$P_{Single} \approx erf\left[\frac{1}{\Gamma_{IM}\sqrt{2}}\right] \quad (9)$$

where erf[·] is the error function.

So far, the probability at a single time slot has been discussed. Signal detections of successive time slots are required for intercepting the data or the key. The probability in such cases is expressed using a successive number *l* as

$$P_{key} = \left(P_{single}\right)^{l} \quad (10)$$

The successive number *l* is related to the key and the mathematical complexity, which is beyond the scope of this work. Figure 5 shows the probability of correct guessing of successive time slots. A higher masking number and a longer *l* are necessary for high security of the system.

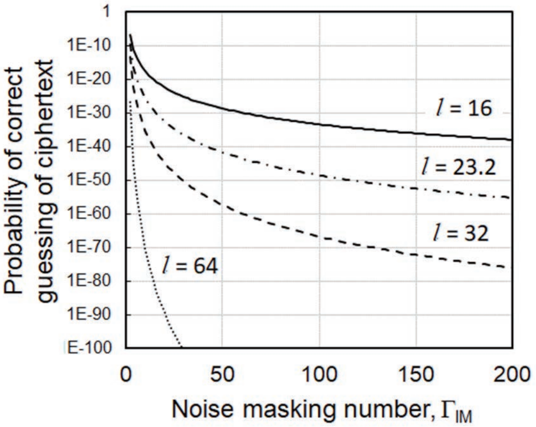

Fig. 5. Probability of correct guessing of ciphertext.

l = 23.2 is the case of the Y-00 cipher transceiver [11] where a linear feedback shift register (LFSR) is employed as a simple pseud-random number generator for mathematical complexity. Even with such simple generator, the probability achieved by the shot noise masking is ~10^{-25} for the parameters of $\lambda = 1550$ nm, max-to-min power ratio r = 2, signal bandwidth R = 1.5 GHz, number of bases $M = 2^{11}$, signal power of 1 mW, and key length of 256 bits. The probability can be easily decreased by employing a higher number of bases. It can also be reduced if a more complicated PRNG is utilized instead of the LFSR.

It should be noted that the entire secrecy of a Y-00 cipher is not only evaluated by the noise masking number. The complexity of the mathematical randomization, namely, the generation scheme of the pseudo random number, must also be considered. However, the above secrecy analysis estimates the fixed number, which is easy to compare.

IV. Conclusion

We have investigated a noise masking effect generated by shot noise for an IM Y-00 cipher. An analytical solution of the noise masking is derived. Next, a probability of correct guessing of the ciphertext by an eavesdropper for an IM Y-00 cipher is investigated, and an approximate analytical solution of the probability, which is expressed by the number of bases and the noise masking number, is derived. The solution is applied to calculate the probability of our IM Y-00 cipher transceiver. The derived solution is useful to evaluate the Y-00 cipher secrecy realized by shot noise. A future issue is to consider the mathematical complexity and other kinds of noise for estimating the entire secrecy of the Y-00 cipher.

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] 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.

[5] 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.

[6] 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.

[7] F. Futami, K. Tanizawa, K. Kato, and O. Hirota, "1,000-km transmission of 1.5-Gb/s Y-00 quantum stream cipher using 4096-level intensity modulation signals," Tech. Dig., Conference on Lasers and Electro - Optics (CLEO 2019), SW3O.4, 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] O. Hirota, "Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol," Phys. Rev. A, 76, 032307, 2007.

[10] 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," SPIE Proc. 1077114, 2018.

[11] 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," SPIE Proc. 99800O, 2016.