ISSN 2186-6570

Quantum-Noise Signal Masking at Microwave Frequency in PSK Y-00 Quantum Stream Cipher System with Optical Heterodyne

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.10, No.1, 9-12, 2020

Quantum-Noise Signal Masking at Microwave Frequency in PSK Y-00 Quantum Stream Cipher System with Optical Heterodyne

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 quantitative analysis of signal masking by quantum (shot) noise at a microwave frequency in PSK Y-00 quantum stream cipher system with optical-to-microwave frequency conversion. The frequency conversion is achieved by optical heterodyne process with local oscillator light. As the amount of shot noise is related to an optical frequency before the conversion, sufficient signal masking by shot noise is achieved at a converted microwave frequency. Theoretical study shows that optical power of the cipher in the heterodyne process determines the amount of masking and signal-to-noise ratio of the cipher. This is a tradeoff between the security and signal quality in a secure wireless system with PSK Y-00 cipher. Numerical analysis shows that this tradeoff is mitigated by increasing a bit resolution of phase randomization in the encryption process.**

***Index Terms*— Y-00 quantum stream cipher, secure wireless communication system.**

I. Introduction

Radio intercept is a security risk of wireless communication networks for transmission of important/private information. In current communication systems, conventional digital ciphers based on computational complexity such as the Advanced Encryption Standard are implemented in order to avoid the tapped signals from being successfully analyzed. Other security solutions that directly protect interceptions from the physical layer have been researched recently. Physical layer security based on advanced coding [1] or physical layer encryption (PLE) which utilizes unique signal encoding or scrambling with a private key [2]–[5] have been demonstrated to improve the security of microwave wireless systems.

Here, PLE utilizing signal masking by quantum (shot) noise [6] is focused on. The symmetric key encryption was originally demonstrated as AlphaEta [7] or the Y-00 quantum stream cipher [8] for optical signal transmission. In the encryption, digital data (plaintext) is converted into an extremely high-order optical signal, e.g., a 2^{17} (= 131,072) phase-shift keying (PSK) signal [9], with a pre-shared private key. Provided that the order is sufficiently high, uncertainty caused by shot noise at detection is larger than the signal distance of the high-order signals. This effect is called quantum-noise signal masking or signal masking by shot noise, which imposes unavoidable errors on the signal interception (measurement) without a key by an eavesdropper. Shot noise is an ideal mask to realize secrecy as it is truly random and inherently inevitable at signal detection. The quantum-noise masking provides a lower bound of security. High-speed optical cipher transmission at 10 Gbit/s or more [9]–[14] and compatibility with dense wavelength-division multiplexing (WDM) systems [15],[16] have been demonstrated for secure fiber-optic transmission. The approach is applied to optical wireless transmission as well [17],[18].

The same approach, in which high-order modulation is employed for the signal masking by shot noise, is not simply applicable to the data encryption of microwave wireless systems. Fig, 1 shows the schematic image of coherent states of a signal at an optical frequency of ~200THz and at a microwave frequency of 30 GHz. The gray circle indicates variance of shot noise. The standard deviation of shot noise is proportional to the square root of the signal frequency [11]. Hence, secrecy realized by the masking via shot noise is ~1/100 at a typical microwave frequency for wireless transmission. To improve the secrecy, adding artificial noise with a pseudorandom noise generator has been demonstrated [4],[5].

Recently, we have proposed and demonstrated photonic generation of Y-00 cipher at microwave frequencies [19],[20]. An optical heterodyne with a local oscillator (LO) was utilized to convert an optical frequency of the cipher into an intended microwave frequency for wireless transmission. The microwave frequency was determined as a difference frequency between the optical cipher and LO. As the variance of shot noise was related to the optical frequency in the heterodyne process, sufficient signal masking by shot noise was achieved at the microwave frequency as well. 12-Gbit/s PSK Y-00 cipher was successfully generated at a center frequency of 30 GHz. This technique was applied to an analog radio-over-fiber (RoF) system, and proof-of-concept 12-Gbit/s RoF and wireless transmissions with enhanced security at a physical layer were demonstrated.

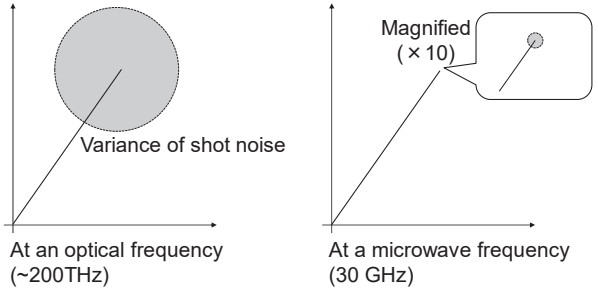

Fig. 1. Quantum (shot) noise of coherent state of optical and microwave signals.

This paper reports theoretical analysis of signal masking by shot noise in a PSK Y-00 cipher system with optical heterodyne process. A quantum-noise masking number which is a primal quantitative measure of security in Y-00 cipher system is derived based on a semi-classical theory of optical heterodyne process. The analysis indicates that the masking number of Y-00 cipher at a microwave frequency is better for lower optical signal power at a photodetector (PD) for heterodyne. On the other hand, the lower signal power reduces signal-to-noise ratio (SNR) of the cipher. The tradeoff between the masking number and SNR is numerically analyzed. The results show that a high masking number which promises high security and high SNR which provides a large system margin for wireless transmission are simultaneously achievable, provided that a bit resolution of phase randomization is a high number of 16 or more.

II. Quantum-Noise Signal Masking At Microwave Frequency

Fig. 2 shows the schematic diagram of PSK Y-00 cipher system with optical heterodyne frequency conversion. PSK Y-00 cipher is generated at an optical frequency of $f_{\text{Y-00}}$. The inset constellation diagrams show the operating principle of the encryption when the data modulation is QPSK (M = 4). Typically, QPSK symbols are mapped to a phase of π/4, 3π/4, 5π/4, or 7π/4 in an I/Q plane, as shown in the left constellation diagram. The arrow on I axis indicates the basis of the phase modulation. The symbols are converted to extremely high-order PSK signals for the encryption. A phase basis angle between –π/4 and π/4 is selected based on a seed key for each symbol. The seed key is pre-shared between legitimate users. When a bit resolution is m, which corresponds to 2^m phase basis angles, the QPSK symbols are mapped to $M{\cdot}2^m$ phase levels. The constellation of PSK Y-00 cipher becomes a shape like a donut, as shown in the right diagram, provided that the bit resolution m is sufficiently high, e.g., 10 bits or more. Such E/O conversion is achieved with a laser and Lithium niobate optical modulators [11].

Then, the cipher is combined with a coherent LO light. The frequency of LO f_{LO} is set to a value such that $f_{\text{RF}} = |f_{\text{Y-00}} - f_{\text{LO}}|$ is satisfied. Here the difference frequency f_{RF} is an intended microwave frequency for wireless communications.

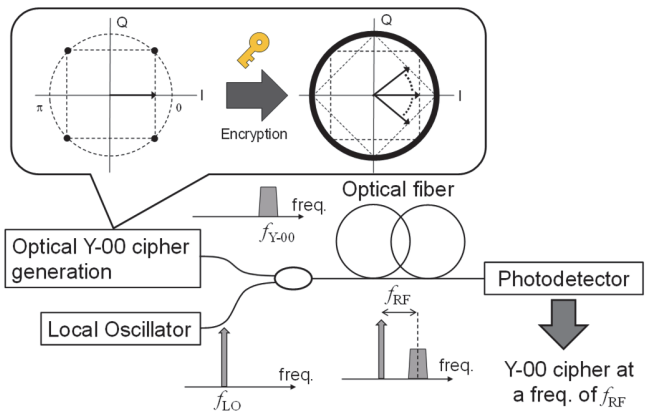

Fig. 2. PSK Y-00 cipher system with optical heterodyne.

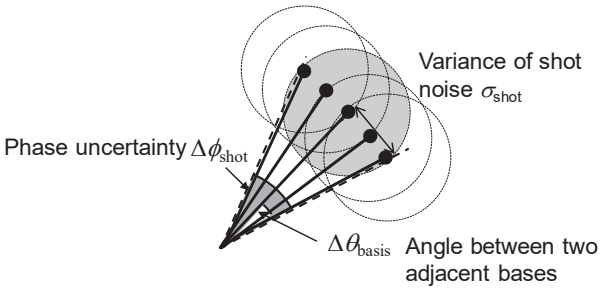

Fig. 3. Magnified image of symbols of PSK Y-00 cipher after heterodyne.

The cipher and LO lights are transmitted over an optical fiber as needed. Finally, E/O conversion is achieved with a PD. A beat component of the cipher and LO lights is generated at f_{RF}. In the following, we theoretically analyze the quantum-noise masking of the microwave cipher generated in this system.

Fig. 3 shows the magnified image of signals in PSK cipher. The gray circle shows a variance of shot noise. Five adjacent signals are masked by the shot noise, which indicates that these five signals can never be detected without errors. A quantum-noise masking number Γ_{Q} is defined as the number of signals masked by the shot noise.

$$\Gamma_{\text{Q}} = \frac{\Delta\phi_{\text{shot}}}{\Delta\theta_{\text{basis}}} \tag{1}$$

Here, $\Delta\phi_{\text{shot}}$ and $\Delta\theta_{\text{basis}}$ are the phase uncertainty caused by shot noise and the angle between adjacent bases, as shown in Fig. 3. The angle $\Delta\theta_{\text{basis}}$ is calculated as

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

where the order of data modulation and the bit resolution of phase randomization are M and m, respectively.

The phase uncertainty $\Delta\phi_{\text{shot}}$ is derived using semi-classical theory of optical heterodyne detection. The variance of shot noise σ_{shot}^2 at ideal heterodyne detection with LO light is calculated as

$$\sigma_{\text{shot}}^2 = 2ei_{\text{bias}}B \tag{3}$$

where e, i_{bias}, and B are the electric charge, bias current of a PD, and electrical signal bandwidth, respectively. The bias direct current is obtained as

$$i_{\text{bias}} = S(P_{\text{S}} + P_{\text{L}}) \tag{4}$$

where S, P_{S}, and P_{L} are the PD responsivity, optical powers of the signal and LO. The optical powers are defined for a single polarization here. The signal current of heterodyne detection i_{sig} is expressed as follows.

$$i_{\text{sig}} = 2S\sqrt{P_{\text{S}} \cdot P_{\text{L}}}\cos[(\omega_S - \omega_L)t + \varphi(t)] \tag{5}$$

Here ω_{S} and ω_{L} are the angular frequency of signal and LO. φ(t) is the modulated phase. A term of phase difference between the signal and LO is omitted here for simplicity. The angle of uncertainty imposed by shot noise $\Delta\phi_{\text{shot}}$, as shown in the magnified image of Fig. 3, is calculated from Eqs. (3)-(5) as follows.

$$\tan\left(\frac{\Delta\phi_{\text{shot}}}{2}\right) \sim \frac{\Delta\phi_{\text{shot}}}{2} = \frac{\sigma_{\text{shot}}}{2S\sqrt{P_S \cdot P_L}} \tag{6}$$

$$\Delta\phi_{\text{shot}} = \sqrt{\frac{2eB}{SP_S}} \tag{7}$$

As the optical power of LO is much larger than the signal power, $P_S + P_L \approx P_L$ is used. The PD responsivity S is calculated as

$$S = \frac{\eta_q e}{h\nu_0} \tag{8}$$

where h, ν_0, and η_q are Planck constant, signal frequency, and quantum efficiency of a PD, respectively. Then, using Eqs (2), (7), and (8), the quantum-noise masking number Γ_Q is obtained.

$$\Gamma_Q = \frac{M \cdot 2^m}{2\pi}\sqrt{\frac{2h\nu_0 B}{\eta_q P_S}} \tag{9}$$

The masking number at a microwave frequency of f_{RF} is calculated by substituting optical power of the cipher at the input of PD into P_S. It is noteworthy that the frequency of ν_0 is an optical frequency of the cipher, not a microwave frequency f_{RF}, which makes the masking number sufficiently high for secrecy. The signal bandwidth B is typically set to a baud rate of the cipher. This equation indicates that the masking number is proportional to 2^m and is inversely proportional to the square root of the optical power of cipher. Hence, it is important to set these two parameters appropriately in this system.

III. Numerical Analysis for System Design

Two key performance indicators of the microwave cipher system are the quantum-noise masking number Γ_Q and SNR of the cipher at f_{RF}. Provided that LO power is much higher than the signal power and that the shot noise is dominant, SNR of heterodyne detection is calculated as follows [21].

$$\text{SNR} = \frac{SP_S}{eB} \tag{10}$$

The SNR of the cipher at the output of PD or just before a wireless link is obtained by substituting optical power of the cipher at the input of PD into P_S. Although other additive noises should be considered as well in a practical system, to discuss the shot-noise limited condition is meaningful because it provides an ultimate performance of the system.

Numerical analysis is performed when the optical power of the cipher at PD and the bit resolution of the phase randomization m are changed. Detailed parameters of the cipher are shown in Table I. Fig. 4 shows the quantum-noise masking number Γ_Q (left vertical axis) and SNR at the output of PD (right vertical axis). As SNR is independent of the bit resolution m, to employ a higher m increases the masking number and improves the security without sacrificing the signal quality. The masking number is inversely proportional to the square root of the optical power, while SNR is proportional to the power. A higher SNR provides a larger system margin of wireless transmission. This tradeoff between the masking number and SNR should be considered carefully when the cipher system is designed. When m = 16 and P_S = –10 dBm, a masking number of more than 150 and SNR of more than 50 dB are achieved. This situation would be an example of a good point of compromise in this cipher system. In addition, it was experimentally demonstrated that a Q penalty for the encryption and decryption was small in this system [20]. Thus this approach is promising for enhancing security at physical layer of a microwave wireless system.

TABLE I
Simulation Parameters in Ultra-long-haul Transmission

Item	Value
Order of data modulation: M	4
Bit number of the resolution of phase randomization: m	12, 14, 16
Bandwidth of cipher: B	6 GHz
Optical frequency of cipher: ν_0	193 THz
Quantum efficiency of PD: η_q	1

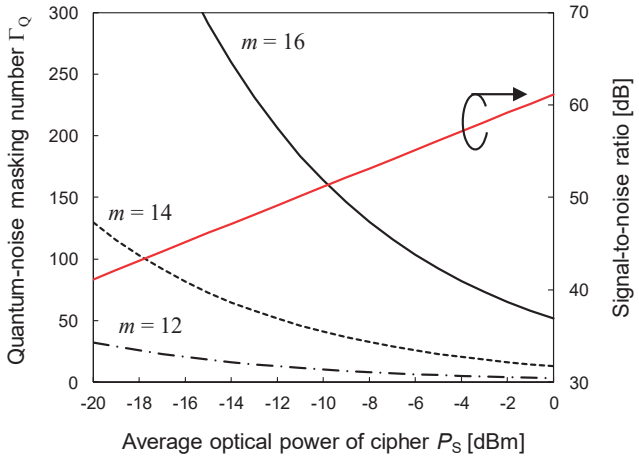

Fig. 4. Quantum-noise masking number and SNR of the cipher at a microwave frequency for various optical powers of the cipher at PD.

IV. Conclusion

We have reported theoretical analysis of signal masking by shot noise in a PSK Y-00 quantum stream cipher system with optical heterodyne frequency conversion. A quantum-noise masking number, which was defined as the number of phase levels covered by shot noise, was determined as a function of optical frequency, optical power, order of data modulation, bit number of bases, and signal bandwidth. We calculated the masking number at a microwave frequency, provided that the order of data modulation and signal bandwidth were 4 (QPSK) and 6 GHz, respectively. The result showed that a masking number of more than 100 was achievable when a bit number of bases is 16 bits or more. A sufficiently high SNR of the cipher at the microwave frequency was achieved as well in the system. Thus PSK Y-00 cipher with optical heterodyne process for the optical-to-microwave frequency conversion is a promising technique for enhancing security at physical layer of microwave wireless systems.

References

[1] V. H. Poor, and F. R. Schaefer, "Wireless physical layer security," *Proc. Natl. Acad. Sci. USA*, vol. 114, no. 1, pp.19-26, 2017.

[2] M. A. Khan, M. Asim, V. Jeoti, and R. S. Manzoor, "On secure OFDM system: Chaos based constellation scrambling," in *Proc. International Conference on Intelligent and Advanced Systems*, pp. 484–488, 2007.

[3] A. Morales, R. Puerta, S. Rommel, and T. I. Monroy, "1 Gb/s chaotic encoded W-band wireless transmission for physical layer data confidentiality in radio-over-fiber systems," *Opt. Express*, vol. 26, no. 17, pp. 22296–22306, 2018.

[4] D. Reilly, and G. Kanter, "Noise-enhanced encryption for physical layer security in an OFDM radio," in *Proc. IEEE Radio and Wireless Symposium (RWS 2009)*, TU2P-28, 2009.

[5] R. Ma, L. Dai, Z. Wang, and J. Wang, "Secure communication in TDS OFDM system using constellation rotation and noise insertion," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1328–1332, 2010.

[6] G. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," *Phys. Rev. Lett.*, vol. 90, p. 227901, 2003.

[7] 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*, vol. 71, no. 6, p. 062326, 2005.

[8] 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*, vo. 72, no, 2, p. 022335, 2005.

[9] K. Tanizawa, and F. Futami, "Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels," *Opt. Express*, vol. 27, no. 2, pp. 1071-1079, 2019.

[10] K. Tanizawa, and F. Futami, "Digital coherent 20-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 800-km SSMF," in *Proc. Optical Fiber Communications Conference (OFC 2019)*, Th1J.7, 2019.

[11] 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, no. 18, pp. 25357-25363, 2019.

[12] K. Ohhata, O. Hirota, M. Honda, S. Akutsu, Y. Doi, K. Harasawa, and K. Yamashita, "10-Gb/s Optical Transceiver Using the Yuen 2000 Encryption Protocol," *J. Lightwave Technol.*, vol. 28, no. 18, pp. 2714-2723, 2010.

[13] K. Tanizawa, and F. Futami, "2^{14} intensity-level 10-Gbaud Y-00 quantum stream cipher enabled by coarse-to-fine modulation," *IEEE Photon. Tech. Lett.*, vol. 30, no. 22, pp.1987-1990, 2018.

[14] M. Nakazawa, M. Yoshida, T. Hirooka, K. Kasai, T. Hirano, T. Ichikawa, and R. Namiki, "QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution," *IEEE J. Quantum Electron.*, vol. 53, no. 4, p. 8000316, 2017.

[15] 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. 2014 OptoElectronics and Communications Conf. and Australian Conf. Optical Fibre Tech. (OECC/ACOFT2014)*, MO1A2, 2014.

[16] 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," *Opt. Express*, vol. 25, no. 26, pp. 33338-33349, 2017.

[17] F. Futami, and O. Hirota, "Demonstration of 2.5 Gbit/sec free space optical communication by using Y-00 cipher: toward secure aviation systems," Proc. SPIE 9202, Photonics Applications for Aviation, Aerospace, Commercial, and Harsh Environments V, 92020R, 2014.

[18] F. Futami, K. Tanizawa, A. Bekkali, and H. Fujita, "Secure Free-Space Optical Transmission of Y-00 Quantum Stream Cipher with 4096-Level Intensity Modulated Signals," in *Proc. 14th Pacific Rim Conference on Lasers and Electro-Optics (CLEO-PR 2020)*, 2020.

[19] K. Tanizawa, and F. Futami, "Photonic Generation of Quantum Noise Assisted Cipher at Microwave Frequencies for Secure Wireless Links," in *Proc. Optical Fiber Communications Conference (OFC 2020)*, M4A.3, 2020.

[20] K. Tanizawa, and F. Futami, "Quantum Noise-Assisted Coherent Radio-over-Fiber Cipher System for Secure Optical Fronthaul and Microwave Wireless Links," *J. Lightwave Technol.*, vol. 38, no. 16, pp. 4244-4249, 2020.

[21] M. C. Teich, "Multiphoton Optical Heterodyne Detection," *IEEE J. Quantum Electron.*, vol. QE-11, no. 8, pp. 595-602, 1975.