ISSN 2186-6570

Effect of Additive Noise on Signal Masking in Microwave OFDM Quantum-Noise Randomized PSK/QAM Encryption

Ken Tanizawa and Fumio Futami

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

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.12, No.1, 7-10, 2022

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.12 No.1 : 7−10 (2022)

Effect of Additive Noise on Signal Masking in Microwave OFDM Quantum-Noise Randomized PSK/QAM Encryption

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

Abstract—**This paper reports analysis of signal masking by quantum (shot) and additive noises in an intensity modulation/direct detection IF-over-fiber system for quantum-noise randomized cipher generation at a microwave intermediate frequency (IF). We investigate a noise masking number of orthogonal frequency-division multiplexing phase-shift keying-/quadrature amplitude modulation-based ciphers, considering the distortion noise of a digital-to-analog converter (DAC) and the classical intensity noise of a laser source. Numerical study shows that the laser intensity noise as well as quantum noise contributes to the signal masking for security against interception in a practical system configuration.**

Index Terms— **stream cipher, secure wireless systems.**

I. Introduction

Wireless technology is rapidly evolving toward 6G network infrastructures. Security enhancement is a major challenge for expanding 6G use cases to solve social issues. In current wireless systems, symmetric-key algorithms, such as the Advanced Encryption Standard (AES), are utilized to protect important/private data from being intercepted. Cryptanalysis, which deduces the plaintext and/or key from the ciphertext without a private key, is difficult to be achieved because of high computational complexity. In addition to the evolution of symmetric-key algorithms, new security measures are expected to implement in the physical layer. Physical layer security (PLS) that utilizes advanced coding [1] for the advantage of a legitimate receiver and physical layer encryption (PLE) that utilizes unique signal encoding or scrambling with a private seed key [2]-[9] have been demonstrated. These approaches achieve signal security, where illegitimate signal reception is directly prevented.

We have demonstrated photonic-assisted PLE utilizing signal masking by quantum (shot) noise for secure wireless communications [6]-[9]. The scheme is based on quantum-noise randomized stream cipher proposed for optical communications, known as AlphaEta [10],[11] or Y-00 quantum stream cipher [12]. A prescribed protocol with a private seed key converts binary data (plaintext) to extremely high-order optical signals. The modulation order after the encryption is sufficiently high, such that quantum noise prevents error-free signal discrimination. Quantum noise is an ideal mask for the signal security because it is truly random and inherently inevitable at detection. The lower bound of security is promised based on the signal masking by quantum noise. Then, the optical encrypted signals are converted to microwave signals through heterodyne process. Quantum noise is naturally added to the microwave signals, resulting in the signal security based on true randomness of quantum mechanics even in microwave frequencies. The effect of quantum noise on a signal is inversely proportional to carrier frequency. Hence, direct high-order microwave signal generation cannot achieve such unique signal security. The photonic-assisted scheme fills the wide frequency gap and expands the applications of quantum-noise randomized stream ciphers.

We experimentally demonstrated mmWave quantum-noise randomized PSK cipher generation via an analog coherent radio-over-fiber (RoF) transmission system [6]. We then proposed a simpler system configuration utilizing an analog intensity modulation/direct detection (IM/DD) intermediate frequency-over-fiber (IFoF) system [7]. The system employed orthogonal frequency-division multiplexing (OFDM) which can cope with severe wireless channels. We experimentally demonstrated the generation of OFDM quantum-noise randomized PSK/QAM ciphers at an intermediate frequency (IF) of a few GHz [7]-[9]. Furthermore, our previous study reported analysis of signal masking by quantum noise in the IM/DD IFoF system for the cipher generation [13]. The role of quantum noise on the security of the system is particularly important, as briefly mentioned above. On the other hand, classical noise is added to the encrypted signals because of practical hardware limitations. The additive noise contributes to the signal masking in practice as long as it is considered to be random. This paper reports the analysis of distortion noise of a digital-to-analog converter (DAC) and intensity noise of a laser source in an analog IM/DD IFoF system for microwave cipher generation. The effect of the additive noise on the signal masking in OFDM quantum-noise randomized PSK/QAM encryption are numerically investigated.

II. Quantum and Additive Noises in Analog IM/DD IF-Over-Fiber Cipher Transmission

Fig. 1 shows the configuration of an analog IM/DD IFoF system for the delivery and generation of microwave encrypted signals. First, high-order electrical baseband signals are generated from data and a seed key. A low-order data modulation, such as QPSK and 16QAM, is converted to high-order PSK/QAM using a prescribed encryption protocol [14],[15]. Next, the encrypted baseband signals are digitally

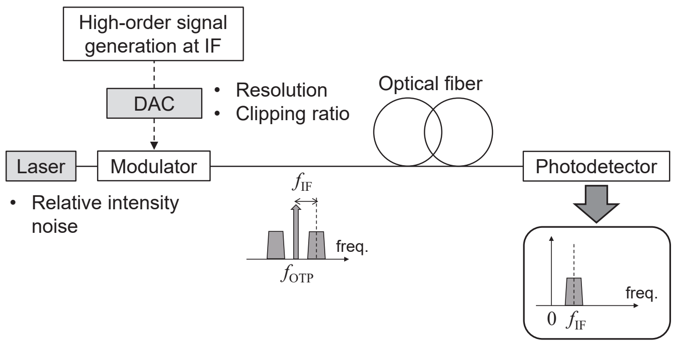

Fig. 1. Quantum-noise randomized cipher generation via analog IM/DD IFoF transmission.

upconverted to an IF f_{IF}. Then, optical intensity is modulated with the IF signals through a DAC. The DAC has a limited resolution, and analog electrical output is distorted. The distortion noise of a DAC is discussed in the following subsection II A. The analog signals modulate optical intensity from a laser source operating at f_{OPT}. The modulation is achieved with a combination of a continuous wave laser source and an optical intensity modulator [7],[8], or with a directly modulated laser diode (DML) [9]. Output power fluctuation of the laser is another source of additive noise in the system, which will be discussed in II B. After fiber transmission, the optical signals are detected with a photodetector, generating encrypted signals at f_{IF}. As the optical carrier frequency is high, sufficient amount of quantum noise for masking adjacent signals is added to the IF signals. Thus, signal encryption for preventing error-free signal interception is achieved. The variance of quantum noise σ^2_{shot} is obtained as,

$$\sigma^2_{\text{shot}} = 2ei_{\text{bias}}B, \tag{1}$$

where e, i_{bias}, and B are electric charge, bias current, and receiver bandwidth, respectively. The bias current is expressed as,

$$i_{\text{bias}} = SP_0, \tag{2}$$

$$S = \frac{\eta_q e}{h\nu_0}, \tag{3}$$

where S, P_0, h, ν_0, and η_q are the responsivity of a photodetector, average optical power, Planck constant, optical carrier frequency, quantum efficiency of a photodetector, respectively. The effect of quantum noise on the signal security is quantitatively discussed in our previous study [13].

A. Distortion noise of DAC

The limited resolution of a DAC induces quantization and clipping, and electrical output signal for optical modulation is distorted. The distortion noise depends on the bit resolution of a DAC and clipping ratio. Quantitative analysis of the noise in an analog IM/DD optical OFDM transmission system was reported in [16]. Using the formulas provided in the paper, we numerically analyze the variance of the distortion noise of a DAC σ^2_{dac} for different bit resolutions. The signal bandwidth B, responsivity of a photodetector S, and optical received power P_0 are set to 1.25 GHz, 0.84 A/W, and 0 dBm, respectively. Fig. 2 shows the variance of quantum (dashed line) and distortion noises (solid line) for different clipping ratios. The clipping ratio is defined as $V_{dac}^2/\sigma^2_{signal}$ where V_{dac} and σ_{signal} are the half of the voltage swing of a DAC and standard deviation of electrical signal, respectively. The bit resolution of a DAC is set to 8, 10, 12, 14, and 16 bits. The optical modulation index (OMI) is 12 %. The results show that quantum noise is dominant for the clipping ratio of more than 11.5 dB and bit resolution of 10 bits or higher. The bit resolution of a high-speed DAC with analog bandwidth of a few GHz is 10 bits or higher. The clipping ratio is typically set approximately at 13 dB. Hence, quantum noise σ^2_{shot} is dominant under such a practical condition.

Fig. 3 shows the variance of quantum (dashed line) and distortion noises (solid line) for different OMIs. The bit resolution of a DAC is set to 8, 10, 12, 14, and 16 bits. The clipping ratio is set at 13 dB. The results show that quantum noise is dominant for the bit resolution of 10 bits or higher. In the proposed IM/DD IFoF system for cipher generation, OMI is a parameter that determines the tradeoff between the signal quality and security: higher signal-to-noise ratio is achieved at a higher OMI while higher signal security is achieved at a lower OMI. Considering the tradeoff, we typically set OMI to ~10 %. Thus, the distortion noise of DAC σ^2_{dac} is suppressed an order of magnitude lower than quantum noise σ^2_{shot} in a practical system configuration.

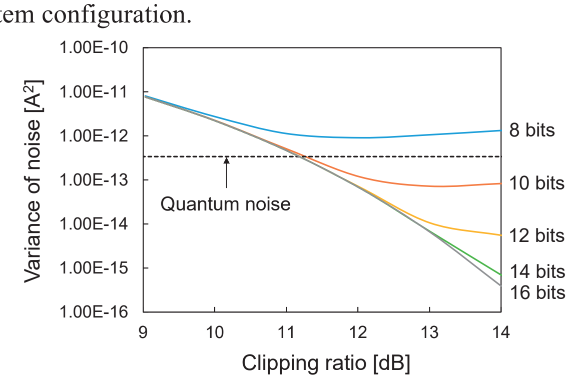

Fig. 2. Variance of quantum and distortion noises for different clipping ratios. The bit resolution of DAC is set to 8, 10, 12, 14, and 16 bits. OMI is 12 %.

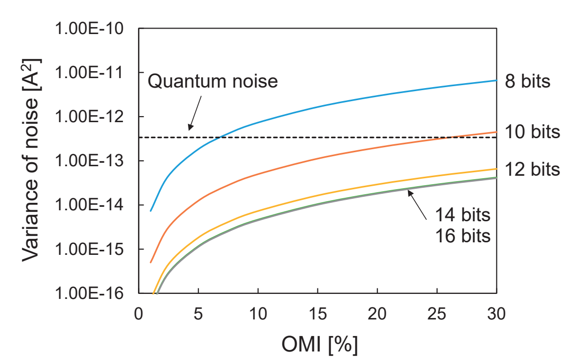

Fig. 3. Variance of quantum and distortion noises for different OMIs. The bit resolution of DAC is set to 8, 10, 12, 14, and 16 bits. The clipping ratio is 13 dB.

B. Intensity noise of laser

The power fluctuation of a laser source also affects the performance of the system. Relative intensity noise (RIN) is used to quantitatively discuss the fluctuation. The variance of laser intensity noise is given as

$$\sigma_{\text{laser}}^2 = \text{RIN} \cdot i_{\text{bias}}^2 B. \quad (4)$$

The noise variance increases as the square of the bias current or optical power, which is typical characteristics of additive classical noise. Fig. 4 shows the variance of quantum (dashed line), DAC distortion (solid line), and laser intensity (chain line) noises for different optical powers. RIN of the laser is set to −155 dB/Hz in this estimation. The bit resolution of DAC is set to 8, 10, 12, 14, and 16 bits. The clipping ratio and OMI are 13 dB and 12 %, respectively. The optical power is related to the tradeoff between the signal quality and security. In most cases, the optical received power is around 0 dBm. This indicates that quantum noise is comparable with the classical intensity noise in the encrypted microwave signal.

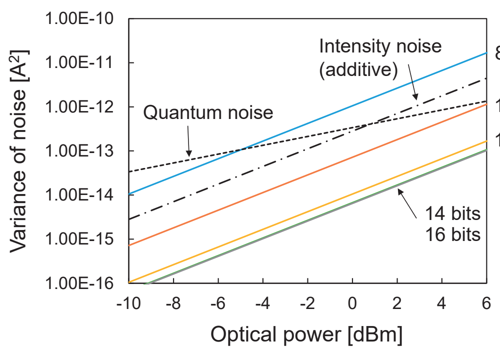

Fig. 4. Variance of quantum, DAC distortion, and laser intensity noises for different optical powers. RIN is set to -155 dB/Hz. The bit resolution of DAC is set to 8, 10, 12, 14, and 16 bits. The clipping ratio and OMI are 13 dB and 12 %, respectively.

III. Quantum- and Additive-Noise Signal Masking

A quantum-noise masking number Γ_Q, defined as the number of signals masked by quantum noise, is a primary measure of signal security. The number is directly related to a lower bound of uncertainty imposed on illegitimate signal detection without a private key. The formulas for calculating the masking number of OFDM PSK/QAM cipher at IF was derived in [13]. Here we consider not only quantum noise but also additive noise and analyze a masking number including the effect of both noises Γ_{all}. The variance of sum of quantum and additive noises is given by

$$\sigma_{\text{all}}^2 = \sigma_{\text{shot}}^2 + \sigma_{\text{dac}}^2 + \sigma_{\text{laser}}^2. \quad (5)$$

The signal masking via additive noise also imposes detection uncertainty and provides signal security as long as the noise is random. In practice, it is meaningful to discuss the signal masking via all noises. On the other hand, the additive noise is not truly random in a strict sense. Hence, it is difficult to exclude the possibility that an eavesdropper reduces the effect of additive noise on illegitimate signal reception. Even in such a case, the signal masking by quantum noise remains, and signal security is maintained in the system.

A. PSK-based Encryption

By replacing σ^2_{shot} with σ^2_{all} in the formulas provided in [13], we obtain the noise masking number for OFDM PSK-based cipher at IF $\Gamma_{\text{all\_psk}}$ as follows:

$$\Gamma_{\text{all\_psk}} = \frac{M \cdot 2^m \cdot \sigma_{\text{all}}}{\sqrt{2\pi} S P_0 \mu_{\text{rms}}}, \quad (6)$$

where M, m, and μ_{rms} are the order of data modulation, the bit resolution of phase randomization, and OMI, respectively. Using Eq. (6), we calculate the noise masking number for various optical powers. Table I summarizes the parameters of the PSK-based cipher. The order of data modulation M and bit resolution for the encryption m are set to 4 (QPSK) and 14, respectively. The order of PSK after the encryption corresponds to 2^{16}. The other parameters, such as the signal bandwidth and OMI, are the same as the ones in the noise analysis shown in Fig. 4. Fig. 5 shows the masking numbers for only quantum noise (dashed line) and quantum and additive noises (solid line). When the bit resolution of DAC is 10 bits or higher, the effect of the DAC distortion noise on the masking number is suppressed. As can be estimated from the results in Sec. II, quantum and laser intensity noises are main factors that contribute to the masking number. The masking numbers at 0 dBm are 85 and 115 for only quantum noise and all noises with a DAC resolution of 16 bits, respectively. Thus, a sufficient amount of quantum noise contributes to the signal masking in a practical situation, ensuring the lower bound of signal security.

TABLE I
Simulation Parameters in PSK-based Cipher

Item	Value
Order of data modulation: M	4
Bit number of the resolution of phase randomization: m	14
Bandwidth of cipher: B	1.25 GHz
Responsivity of PD: S	0.84 A/W
Clipping ratio	13 dB
OMI (rms): μ_{rms}	0.12

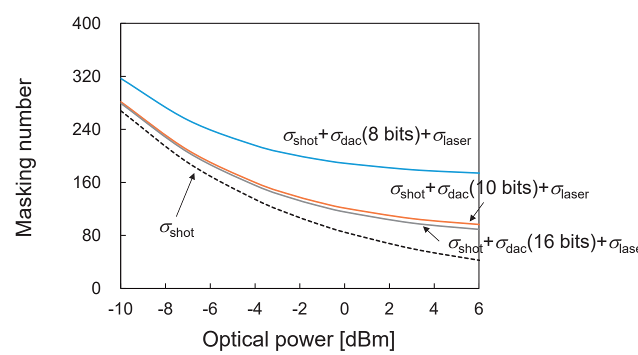

Fig. 5. Noise masking numbers for different optical powers in an IM/DD IFoF system for microwave PSK-based cipher generation.

B. QAM-based Encryption

The noise masking number for OFDM QAM-based cipher at IF $\Gamma_{\text{all\_qam}}$ is obtained similarly based on our previous study [13]:

$$\Gamma_{\text{all\_qam}} = \frac{\pi (M \cdot 2^{2m} - 1) \sigma_{\text{all}}^2}{12 S^2 P_0^2 \mu_{\text{rms}}^2}. \quad (7)$$

Table II shows the parameters of QAM-based cipher in the following numerical analysis. The order of data modulation M

and bit resolution for the encryption of each I/Q amplitude *m* are set to 16 (16 QAM) and 10, respectively. The encrypted signal follows a 2^{24} QAM template. The other parameters are the same as the ones in the noise analysis shown in Fig. 4. Fig. 6 shows the masking numbers for only quantum noise (dashed line) and quantum and additive noises (solid line). As is the cases of PSK-based cipher, quantum and laser intensity noises are dominant provided that a DAC resolution is 10 bits or higher. The masking numbers at 0 dBm are 145 and 268 for only quantum noise and all noises with a DAC resolution of 16 bits, respectively. Quantum noise provides a significant contribution to the signal security.

TABLE II
SIMULATION PARAMETERS IN QAM-BASED CIPHER

Item	Value
Order of data modulation: M	16
Bit number of the resolution of amplitude randomization for each I or Q component: : m	10
Bandwidth of cipher: B	1.25 GHz
Responsivity of PD: S	0.84 A/W
Clipping ratio	13 dB
OMI (rms): μ_{rms}	0.12

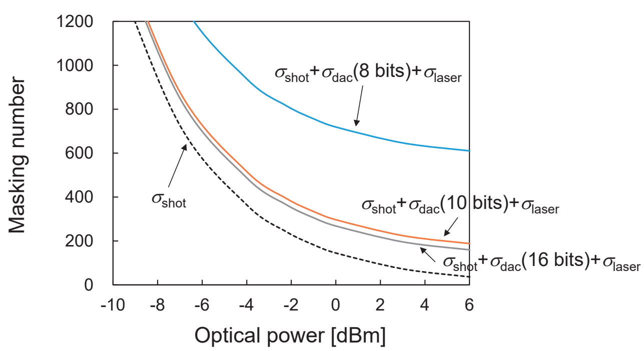

Fig. 6. Noise masking numbers for different optical powers in an IM/DD IFoF cipher system based on QAM.

IV. CONCLUSION

We discussed the effect of quantum and additive noises on signal masking in a microwave OFDM quantum-noise randomized PSK/QAM encryption system via analog IM/DD IFoF transmission. The additive noise includes distortion noise of a DAC and intensity noise of a laser. Numerical study with practical system parameters showed that the distortion noise was fully suppressed provided that the bit resolution of a DAC and clipping ratio were 10 bits and 13 dB, or higher, respectively. The classical laser intensity noise and quantum noise mainly contributed to the signal masking in a practical range of received optical power. The intensity noise from the laser imposes uncertainty on illegitimate signal reception and improves the signal security. On the other hand, quantum noise which is truly random and irreducible ensures the lower bound of signal security in the system.

ACKNOWLEDGMENT

This work was supported in part by JSPS KAKENHI Grant Number JP21H01329 and the SECOM Science and Technology Foundation.

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] 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.

[7] K. Tanizawa, and F. Futami, "IF-over-Fiber Transmission of OFDM Quantum-Noise Randomized PSK Cipher for Physical Layer Encryption of Wireless Signals," *J. Lightwave Technol.*, vol. 40, no. 6, pp. 1698-1704, 2022.

[8] K. Tanizawa, and F. Futami, "Analog IM/DD IFoF Transmission of OFDM Quantum-Noise Randomized QAM Cipher for Wireless Signal Encryption," in *Proc. 27th Opto-Electronics and Communications Conference (OECC/PSC 2022)*, TuF2-3, 2022.

[9] K. Tanizawa, and F. Futami, "Microwave OFDM Quantum-Noise Randomized QAM Cipher Generation via Analog IFoF Transmission with a DML," in *Proc. 48th European Conference on Optical Communications (ECOC 2022)*, Tu5.57, 2022.

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

[11] 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.

[12] 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.

[13] K. Tanizawa, and F. Futami, "Quantum-Noise Signal Masking of OFDM PSK/QAM Quantum-Noise Randomized Ciphers in IM/DD IF-over-Fiber Systems," *Tamagawa University Quantum ICT Research Institute Bulletin*, vol. 11, no. 1, pp. 1-5, 2021.

[14] K. Tanizawa, and F. Futami, "Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system," *Opt. Express*, vol. 29, no. 7, pp. 10451-10464, 2021.

[15] X. Chen, K. Tanizawa, P. Winzer, P. Dong, J. Cho, F. Futami, K. Kato, A. Melikyan, and KW Kim, "Experimental demonstration of 4,294,967,296-QAM based Y-00 quantum stream cipher template carrying 160-Gb/s 16-QAM signals," *Optics Express*, vol. 29, no. 4, pp. 5658-5664, 2021.

[16] E. Vanin, "Performance evaluation of intensity modulated optical OFDM system with digital baseband distortion," *Opt. Express*, vol. 19, no. 5, pp. 4280-4293, 2011.