ISSN 2186-6570

Quantum-Noise Signal Masking of OFDM PSK/QAM Quantum-Noise Randomized Ciphers in IM/DD IF-over-Fiber Systems

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.11, No.1, 1-5, 2021

Quantum-Noise Signal Masking of OFDM PSK/QAM Quantum-Noise Randomized Ciphers in IM/DD IF-over-Fiber Systems

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 analysis of signal masking by quantum (shot) noise in an intensity modulation/direct detection IF-over-fiber system for quantum-noise randomized cipher generation at a microwave intermediate frequency (IF). We derive the formula for calculating a quantum-noise signal masking number of orthogonal frequency-division multiplexing phase-shift keying-/quadrature amplitude modulation-based ciphers. The masking number is related to uncertainty imposed on the illegitimate detection of the cipher and is a primal security measure. The formula indicates that the bit resolution of signal randomization in the encryption, optical received power, and modulation index are important design parameters. Numerical study shows that more than a few tens of masking number is achievable for encrypted microwave signal at 5 Gbit/s.**

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

I. Introduction

Wireless networks are an essential infrastructure for communications. Radio intercept is a security risk of wireless communication systems. In the current systems, conventional ciphers based on computational complexity such as the Advanced Encryption Standard (AES) are utilized to protect important/private data from being intercepted. AES is a block cipher with a private seed key and converts a plaintext to a ciphertext digitally. Cryptanalysis, which deduces the plaintext and/or key from the ciphertext without the private key, is difficult because of the high computational complexity. To further improve the security against wireless interception, physical layer security 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]–[6] have been researched. Illegitimate signal reception itself is directly prevented in these approaches.

We have proposed and demonstrated PLE utilizing signal masking by quantum (shot) noise for wireless communications [6]. The symmetric key encryption was originally demonstrated as AlphaEta [7,8] or the Y-00 quantum stream cipher [9] for optical communications. A plaintext which is binary data is converted into an extremely high-order optical signal, e.g., a 2^{17} (= 131,072) phase-shift keying (PSK) signal [10], with a private seed key. Provided that the order is sufficiently high, uncertainty caused by quantum (shot) noise prevents error-free signal discrimination. This effect is called quantum-noise signal masking or signal masking by quantum noise. Quantum noise is an ideal mask to achieve secrecy because it is truly random and inherently inevitable at signal detection.

We extended the scheme to wireless communications. To solve the issue of insufficient quantum-noise signal masking in microwave frequencies which are three to five orders of magnitude lower than an optical frequency of ~200 THz, a microwave photonics technology was utilized. First, a high-order signal was generated at an optical frequency. Next, the optical signal was mixed with a local oscillator (LO) light whose frequency was shifted from the optical signal frequency. The frequency difference was set to the value of an intended microwave frequency for wireless communications. Then, two lights were detected simultaneously with a photodetector, generating a high-order microwave signal with sufficient signal masking by quantum noise. We experimentally demonstrated 12-Gbit/s PSK-based quantum-noise randomized cipher generation at a center frequency of 30 GHz and wireless transmission of the cipher [6]. Although the approach directly synthesized mmWave for wireless communications, the radio-over-fiber (RoF) system required an LO light source and complex combination of optical modulators.

Recently, we have proposed an intensity modulation/direct detection (IM/DD) intermediate frequency-over-fiber (IFoF) system for the generation of quantum-noise randomized cipher [11]. The system requires one laser source and one optical intensity modulator, and the configuration is simplified. We also employ orthogonal frequency-division multiplexing (OFDM) which can cope with severe wireless channels. We experimentally demonstrated the generation of 4.09-Gbit/s OFDM PSK-based quantum-noise randomized cipher at an intermediate frequency (IF) of 3.6 GHz. This paper reports analysis of signal masking by quantum noise in the IM/DD IFoF system for cipher generation. Formulas for calculating the quantum-noise masking number which is a primal quantitative measure of security are derived for OFDM PSK- and quadrature amplitude modulation (QAM)-based ciphers. Numerical analysis of 5-Gbit/s PSK/QAM cipher systems with practical design parameters are shown.

II. Quantum-Noise Randomized Cipher via IF-Over-Fiber System

Fig. 1 shows the configuration of an RoF cipher system with optical heterodyne frequency conversion. First, a high-order electrical baseband signal is generated from data and a seed key.

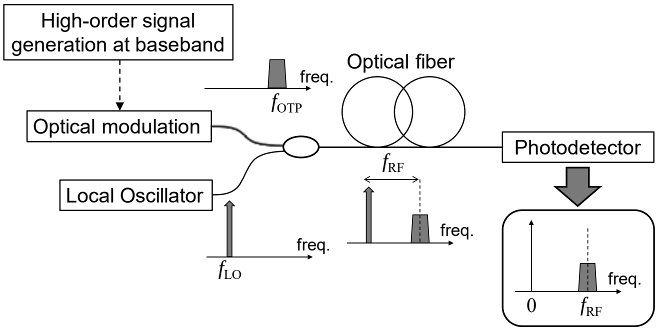


Fig. 1. Quantum-noise randomized cipher generation via analog coherent RoF transmission.

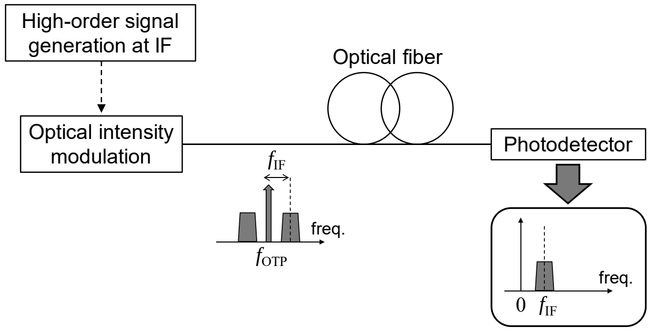


Fig. 2. Quantum-noise randomized cipher generation via analog IM/DD IFoF transmission.

A prescribed protocol is utilized to convert a low-order data modulation, such as BPSK and QPSK, into the high-order signal [12]. Next, optical intensity, phase, or quadrature amplitude modulation is performed, generating an optical high-order signal. Then, the signal is combined with a coherent LO light. The frequency of LO f_{LO} is set to a value such that $f_{\mathrm{RF}} = |f_{\mathrm{OPT}} - f_{\mathrm{LO}}|$ is satisfied. The difference frequency f_{RF} is an intended microwave frequency for wireless communications. The signal and LO lights are transmitted over an optical fiber, followed by E/O conversion with a photodetector. A beat component of the high-order signal and LO lights is generated at f_{RF}. As the amount of quantum noise depends on the optical frequency, sufficient quantum-noise signal masking at f_{RF} for the encryption is achieved. The system requires an IQ modulator or complex combination of modulators for the optical modulation and additional laser source for the LO, while the encrypted signal at a microwave frequency for wireless communications is directly generated.

Fig. 2 shows the configuration of IM/DD IFoF cipher system we recently proposed. First, a high-order electrical signal is generated at an IF of f_{IF}. Then, optical intensity is modulated with the signal. The optical intensity modulation can be achieved with a combination of a continuous wave laser source and a simple optical intensity modulator or with a directly modulated laser diode, which makes the system configuration much simpler. The optical signal is detected with a photodetector after fiber transmission, generating the encrypted signal at f_{IF}. As is the case with the RoF cipher system, sufficient quantum-noise signal masking is achieved because of the high optical carrier frequency. After the detection, frequency up-conversion is performed for wireless communications, as needed.

III. Quantum-Noise Signal Masking

A quantum-noise masking number Γ_{Q} is defined as the number of signals masked by quantum noise. This number is a primary measure of security which indicates unavoidable uncertainty of illegitimate detection without a private seed key. Here we derive the formulas for calculating the masking number of OFDM PSK/QAM ciphers at IF. In the IM/DD IFoF cipher system, the optical power of subcarrier modulated signals $P(t)$ is expressed as:

$$P(t) = P_0\left[1 + \sum_{k=1}^{N} \mu_k\, a_k(t)\cos(\omega_k t + \varphi_k(t))\right], \qquad (1)$$

where P_0 and N are the average optical power and the number of OFDM subcarriers, and μ_{k}, $a_{\mathrm{k}}(t)$, ω_{k}, and $\varphi_{\mathrm{k}}(t)$ are the modulation index, normalized amplitude, angular frequency, and phase of k-th subcarrier, respectively. When the modulation index of each subcarrier is the same, the total modulation index μ_{rms} is expressed as:

$$\mu_{\mathrm{rms}} = \sqrt{\frac{\mu_k^2 \cdot N}{2}}. \qquad (2)$$

The photocurrent is obtained from the optical power as:

$$i(t) = SP_0\left[1 + \sum_{k=1}^{N} \mu_k\, a_k(t)\cos\big(\omega_k t + \varphi_k(t)\big)\right]. \qquad (3)$$

S is the responsivity of a photodetector and expressed as:

$$S = \frac{\eta_{\mathrm{q}}\mathrm{e}}{h\nu_0}, \qquad (4)$$

where h, ν_0, η_{q}, and e are Planck constant, optical carrier frequency, quantum efficiency of a photodetector, and electric charge, respectively. From the photocurrent $i(t)$, the signal current of k-th subcarrier $i_{\mathrm{sig\_k}}$ and bias current i_{bias} are expressed as follows:

$$i_{\mathrm{sig\_k}}(t) = SP_0\mu_k a_k(t)\cos(\omega_k t + \varphi_k(t)), \qquad (5)$$

$$i_{\mathrm{bias}} = SP_0. \qquad (6)$$

From the signal current, the complex amplitude of k-th subcarrier I_{k} at ω_{k} is obtained as follows:

$$I_{\mathrm{k}} = SP_0\mu_k a_k(t)\exp[j\varphi_k(t)]. \qquad (7)$$

The variance of quantum noise $\sigma_{\mathrm{shot}}{}^2$ is calculated from the bias current as:

$$\sigma_{\mathrm{shot}}^2 = 2\mathrm{e}i_{\mathrm{bias}}B, \qquad (8)$$

where B is the receiver bandwidth.

A. PSK-based Encryption

Fig. 3 shows the constellation diagram of PSK-based quantum-noise randomized cipher. The gray circle in the magnified image shows a variance of quantum noise. Five adjacent signals are masked by quantum noise, which indicates that these five signals can never be discriminated without errors. A quantum-noise masking number for the OFDM PSK-based cipher $\Gamma_{\mathrm{Q\_psk}}$ is defined as the ratio of the phase uncertainty caused by quantum noise $\Delta\phi_{\mathrm{shot}}$ to the angle between adjacent signals $\Delta\theta_{\mathrm{basis}}$.

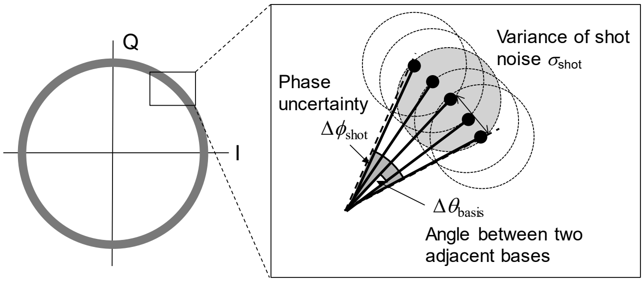

Q
I
Variance of shot noise σ_{shot}
Phase uncertainty
$\Delta\phi_{\text{shot}}$
$\Delta\theta_{\text{basis}}$
Angle between two adjacent bases

Fig. 3. Constellation diagram of PSK-based quantum-noise randomized cipher.

$$\Gamma_{\text{Q\_psk}} = \frac{\Delta\phi_{\text{shot}}}{\Delta\theta_{\text{basis}}}. \tag{9}$$

The angle $\Delta\theta_{\text{basis}}$ is calculated as:

$$\Delta\theta_{\text{basis}} = \frac{2\pi}{M \cdot 2^m}, \tag{10}$$

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

The angle uncertainty imposed by quantum noise $\Delta\phi_{\text{shot}}$, as shown in the magnified image of Fig. 3, is calculated from Eqs. (6)-(8) as follows:

$$\tan\left(\frac{\Delta\phi_{\text{shot}}}{2}\right) \sim \frac{\Delta\phi_{\text{shot}}}{2} = \frac{\sigma_{\text{shot}}}{\overline{|I_{\text{k}}|}}, \tag{11}$$

$$\Delta\phi_{\text{shot}} = \sqrt{\frac{8\text{e}B_{\text{s}}}{SP_0\mu_k^2 N}}. \tag{12}$$

Here we substitute B_{s}/N for B in Eq (8) where B_{s} is the total signal bandwidth. As the amplitude of PSK signal is constant, $\overline{|a_k(t)|} = 1$. Then, using Eqs (2), (4), (9), (10), and (12), the quantum-noise masking number $\Gamma_{\text{Q\_psk}}$ is obtained as:

$$\Gamma_{\text{Q\_psk}} = \frac{M \cdot 2^m}{\pi}\sqrt{\frac{h\nu_0 B_{\text{s}}}{\eta_{\text{q}} P_0 \mu_{\text{rms}}^2}}. \tag{13}$$

It is noteworthy that the frequency of ν_0 is an optical frequency, not a microwave frequency, which makes the masking number sufficiently high for secrecy. This equation indicates that the masking number is proportional to 2^m and inversely proportional to the square root of the received optical power.

B. QAM-based Encryption

Fig. 4 shows the constellation diagram of QAM-based quantum-noise randomized cipher. The number of signals inside the gray circle which indicates a variance of quantum noise is the masking number for QAM-based cipher $\Gamma_{\text{Q\_qam}}$. Provided that the distance between adjacent signals is d in the QAM constellation, the masking number is calculated as:

$$\Gamma_{\text{Q\_qam}} = \pi\frac{\sigma_{\text{shot}}^2}{d^2}. \tag{14}$$

The distance d and average energy per signal of QAM has the following relation [13]:

$$\overline{|I_{\text{k}}|^2} = S^2 P_0^2 \mu_k^2 = \frac{(M \cdot 2^{2m} - 1)d^2}{6}. \tag{15}$$

where $\overline{a_k^2(t)} = 1$ is used. Here, the order of QAM after the encryption is $M \cdot 2^{2m}$, where M and m are the order of data modulation and the bit number of amplitude randomization of in-phase/quadrature component, respectively. The QAM constellation is assumed to be a square shape. Using Eqs. (2), (4), (14), and (15), the making number of QAM-based cipher is obtained as:

$$\Gamma_{\text{Q\_qam}} = \frac{\pi(M \cdot 2^{2m} - 1)h\nu_0 B_{\text{s}}}{6\eta_{\text{q}} P_0 \mu_{\text{rms}}^2}. \tag{16}$$

Here we substitute B_{s}/N for B in Eq (8). The masking number is approximately proportional to 2^{2m} for a large m and inversely proportional to the received optical power.

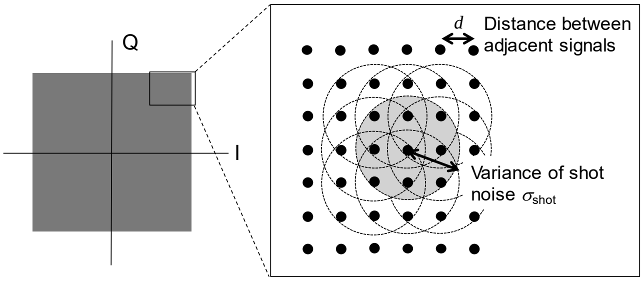

Q
I
d
Distance between adjacent signals
Variance of shot noise σ_{shot}

Fig. 4. Constellation diagram of QAM-based quantum-noise randomized cipher.

IV. Numerical Analysis

We numerically analyze the quantum-noise masking number of PSK and QAM-based cipher at an IF. The important design parameters of the cipher system are the bit resolution of randomization m, optical average received power P_0, and total modulation index μ_{rms}. A typical non-cipher IFoF system employs $\mu_{\text{rms}} \approx 0.3$ to balance linearity of modulation and signal-to-noise ratio. Meanwhile, the modulation index is related not only to the signal quality but also to the masking number or security in the cipher system.

The masking numbers of PSK-based quantum-noise randomized cipher $\Gamma_{\text{Q\_psk}}$ for various total modulation indexes were calculated using Eq. (13). The received optical power P_0 was set to 0 dBm. The other detailed parameters of the cipher for a bit rate of 5 Gbit/s are shown in Table I. Fig. 5 shows the results. The masking number reaches a few tens or higher for a bit resolution of phase randomization m of 14 or more. Although a higher m achieves a higher masking number or security without sacrificing signal quality, the number is limited by the bit resolution of a digital-to-analog converter in practice. To reduce the modulation index μ_{rms} is effective to increase the masking number. As a low μ_{rms} induces the reduction of signal-to-noise ratio, the value should be carefully determined to balance the signal quality and security of the system.

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	12, 14, 16
Bandwidth of cipher: B_{s}	2.5 GHz
Optical frequency of cipher: ν_0	193 THz
Quantum efficiency of photodetector: η_{q}	1

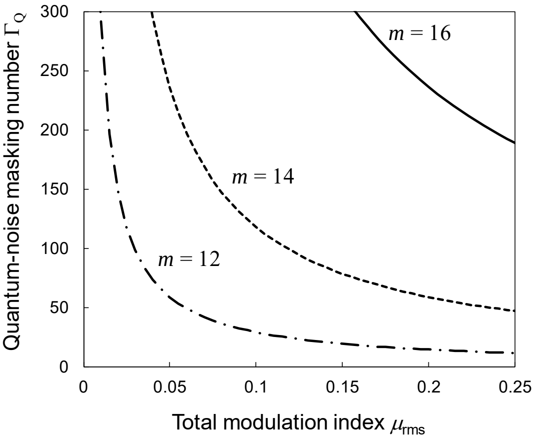
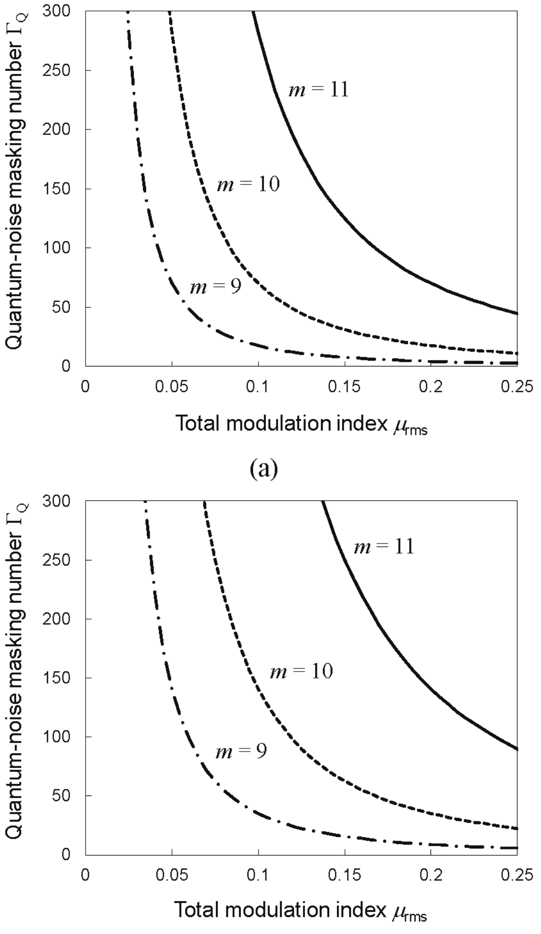


Fig. 5. Quantum-noise masking number of PSK-based cipher with QPSK data modulation.

Next, the masking numbers of QAM-based quantum-noise randomized cipher Γ_{Q_qam} for various total modulation indexes were calculated using Eq. (16). The received optical power P_0 was set to 0 dBm. The other detailed parameters of the cipher are shown in Table II. We calculated two cases for the same bit rate of 5 Gbit/s: QPSK data modulation (M = 4) with a signal bandwidth B_s of 2.5 GHz and 16QAM data modulation (M = 16) with B_s of 1.25 GHz. The bit resolution of amplitude randomization m is defined for in-phase/quadrature component here, and the QAM order after the encryption is $M \cdot 2^{2m}$. Figs. 6(a) and (b) shows the results of QPSK data modulation with B_s = 2.5 GHz and 16QAM data modulation with B_s = 1.25 GHz, respectively. When the results are compared for the same number of bit resolution m, the system with 16-QAM data modulation achieves higher masking numbers because the product of the order of data modulation M and bandwidth B_s increases twofold of the system with QPSK data modulation. However, one cannot simply claim that the system with 16QAM data modulation is better, because the QAM orders after the encryption $M \cdot 2^{2m}$, which are practically limited by the bit resolution of a digital-to-analog converter, are different between them. When the systems are compared for the same QAM order after the encryption $M \cdot 2^{2m}$, e.g. m = 11 for M = 4 vs. m = 10 for M = 16, the system with QPSK data modulation achieves a twofold greater masking number. However, the system with QPSK data modulation needs twofold bandwidth. Thus, the system should be designed considering the practical limitations, such as the bit resolution of a digital-to-analog converter and available signal bandwidth.

TABLE II
SIMULATION PARAMETERS IN QAM-BASED CIPHER

Item	Value
Order of data modulation: M	4, 16
Bit number of the resolution of amplitude randomization for each quadrature: m	9, 10, 11
Bandwidth of cipher: B_s	2.5 GHz for M = 4 1.25 GHz for M = 16
Optical frequency of cipher: ν_0	193 THz
Quantum efficiency of PD: η_q	1



(a)

(b)

Fig. 6. Quantum-noise masking number of QAM-based cipher with (a)QPSK and (b)16QAM data modulations.

III. CONCLUSION

We derived the formula for calculating quantum-noise signal masking number of microwave OFDM PSK/QAM quantum-noise randomized ciphers in the IM/DD IFoF cipher system. The formula indicates that higher masking numbers, which are preferred for high security, are realized provided that the bit resolution of signal randomization is high and that the modulation index is low. To increase the bit resolution is achievable without negative impacts on the signal quality. However, the resolution is practically limited by a digital-to-analog converter. To reduce the modulation index induces the degradation of signal quality. Thus, it is important to determine these parameters appropriately, taking into account the communication system requirements and implementations.

ACKNOWLEDGMENT

The authors thank Prof. K. Kato for fruitful discussion about QAM-based encryption. 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] G. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," *Phys. Rev. Lett.*, vol. 90, p. 227901, 2003.

[8] 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.

[9] 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.

[10] 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.

[11] K. Tanizawa, and F. Futami, "Photonic-Assisted Microwave OFDM Quantum-Noise Randomized Cipher Generation via IM/DD IFoF Transmission," in *Proc. Optical Fiber Communications Conference (OFC 2021)*, Tu5F.7, 2020.

[12] 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.

[13] J. Chesnoy (Editor), "Undersea Fiber Communication Systems 2nd Edition," Elsevier, 2015, pp.63-74.