Quantum Noise-Assisted Coherent Radio-Over-Fiber Cipher System for Secure Optical Fronthaul and Microwave Wireless Links

Ken Tanizawa, *Member, IEEE*, and Fumio Futami, *Member, IEEE*

***Abstract*—This article reports on a symmetric-key direct-data encryption technique that directly protects the interception of optical and microwave signals from physical layer in a coherent analog radio-over-fiber (RoF) system. Secrecy is realized by signal masking by quantum (shot) noise. The quantum noise masking for the encryption is achieved by converting data into extremely high-order signals at an optical frequency. After signal transmission over an optical fronthaul link, the frequency of the encrypted signal is shifted to a microwave frequency via an optical heterodyne process using a local oscillator for wireless transmission. The effect of the quantum noise masking is naturally and seamlessly kept in the heterodyne process. We experimentally demonstrate 12 Gbit/s coherent RoF cipher systems utilizing the quantum noise masking for a 30 GHz wireless band. Adequate signal quality and high security against interception with sufficient quantum noise masking are simultaneously achieved in the optical fronthaul and microwave wireless links.**

***Index Terms*—Communication system security, encryption, microwave photonics, optical fiber communication, RoF systems.**

I. Introduction

HIGH security is a critical value in communication networks for transmission of important/private information. One such security risk is interception in the physical layer of communication systems, such as fiber tapping and radio intercept. Wireless transmission is particularly vulnerable to interception as microwave signals are broadcast through the air. In current systems, conventional ciphers based on computational complexity are implemented in the higher layers to avoid the tapped signals from being successfully analyzed. The interception from the physical layer itself should be directly protected to achieve higher security in communication systems. Recently, security of the physical layer in wireless systems has been researched. Physical layer security based on advanced coding [1] or direct-data encryption for the physical layer, which utilizes unique signal encoding or scrambling [2]–[5], have been demonstrated.

Here, we focus on symmetric-key direct-data encryption utilizing signal masking by quantum (shot) noise [6]. This cipher system was originally demonstrated as AlphaEta [7] or the Y-00 quantum stream cipher [8] for fiber-optic transmission. Secrecy was achieved by converting data (plain text) into an extremely high-order signal with a pre-shared short seed key. The cipher was, for instance, a 2^{17} (=131,072) phase-shift keying (PSK) signal [9]; uncertainty caused by quantum noise at detection was larger than the short signal distance of the high-order signals, and correct measurement of the cipher by an eavesdropper without the key was disrupted. Quantum noise has been an ideal mask to realize secrecy as it is truly random and inherently inevitable. The secrecy realized by quantum noise masking can neither be modified nor avoided. Hence, the security of the system against tapping remains high, even if the computational resources increase drastically. High-speed 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 transmissions.

To utilize quantum noise masking for the encryption of wireless signals is a straightforward extension. However, the effect of the masking cannot be simply extended to wireless frequencies as it is proportional to the square root of the signal frequency. Microwave frequencies (1 to 100 GHz) are typically three to five orders of magnitude lower than the optical one used for communications ($\sim$200 THz). Hence, the secrecy at a frequency of 20 GHz is approximately 1/100 of the one at the optical frequency. Adding artificial noise with a pseudorandom noise generator has been demonstrated [4], [5]. The artificial noise was not truly random, unlike the quantum noise, and the secrecy realized by the masking due to the artificial noise could not be assessed theoretically in a strict sense.

We have recently proposed photonic generation of the quantum noise-masking cipher at microwave frequencies [17]. An optical heterodyne with a local oscillator (LO) was utilized to achieve sufficient signal masking by quantum noise at microwave frequencies. Generation of a 12 Gbit/s quantum noise-masking cipher at a center frequency of 30 GHz was demonstrated. This paper reports secure coherent analog radio-over-fiber (RoF) systems utilizing the photonic generation of the cipher. We experimentally demonstrated a proof-of-concept 12 Gbit/s coherent RoF cipher systems for 30 GHz wireless bands. Sufficient quantum noise masking was achieved both in the optical fronthaul and microwave wireless links, while

Manuscript received November 14, 2019; revised March 30, 2020; accepted April 8, 2020. Date of publication April 20, 2020; date of current version July 28, 2020. This work was supported in part by JSPS KAKENHI under Grant JP18K04290 and Grant JP19K04397 and in part by Telecommunications Advancement Foundation. *(Corresponding author: Ken Tanizawa.)*

The authors are with the Quantum ICT Research Institute, Tamagawa University, Machida 194-8610, Japan (e-mail: tanizawa@lab.tamagawa.ac.jp; futami@lab.tamagawa.ac.jp).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2020.2987213

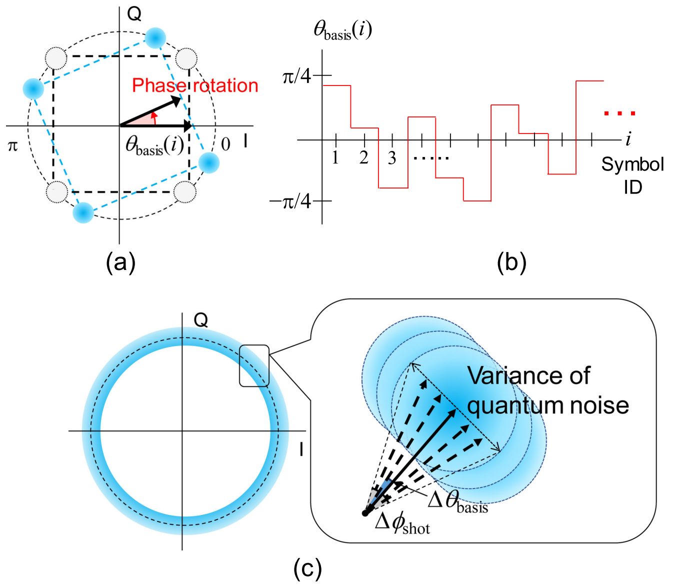
Q
Phase rotation
π
0
I
$\theta_{\text{basis}}(i)$
(a)
$\theta_{\text{basis}}(i)$
$\pi/4$
$-\pi/4$
1
2
3
....
i
Symbol ID
(b)
Q
I
Variance of quantum noise
$\Delta\theta_{\text{basis}}$
$\Delta\phi_{\text{shot}}$
(c)

Fig. 1. Signal masking by quantum noise: (a) Rotation of phase basis of a symbol of QPSK, (b) Symbol-by-symbol change of rotation angles, (c) Constellation diagram after encryption.

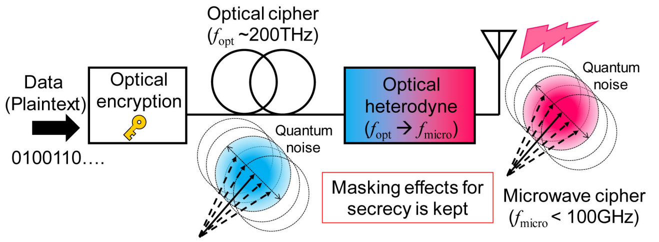
Optical cipher (f_{opt} ~200THz)
Data (Plaintext)
Optical encryption
0100110....
Quantum noise
Optical heterodyne ($f_{\text{opt}} \rightarrow f_{\text{micro}}$)
Quantum noise
Masking effects for secrecy is kept
Microwave cipher (f_{micro} < 100GHz)

Fig. 2. Seamless conversion of the effect of quantum noise masking from optical to microwave frequencies using optical heterodyne techniques.

adequate signal qualities were kept. A coherent RoF system with high security against both fiber tapping and radio intercept was realized. The paper is organized as follows: In Section II, operating principles of the quantum noise-masking cipher and our proposed photonic generation of the cipher at microwave frequencies are explained. In Section III, experimental demonstrations of the 12 Gbit/s RoF cipher for 30 GHz wireless transmission are shown. In Section IV, practical security of the proposed system is discussed. The paper is concluded in Section V.

II. Operating Principles

A. Quantum Noise Making for Secrecy

To exploit signal masking by quantum noise, the basis phase of conventional M-ary phase shift keying (PSK) data modulation was rotated at an extremely high resolution in a symbol-by-symbol manner. A short seed key, which was securely pre-shared between legitimate users, was used to determine the rotation angles. The operating principle of the encryption is explained in Fig. 1. The data modulation was quadrature phase shift keying (QPSK) ($M = 4$). As shown in Fig. 1(a), the phase basis of a symbol of QPSK (the arrow on I axis) was rotated by $\theta_{\text{basis}}(i)$. Here, i is the identification number of a symbol. The rotation angles $\theta_{\text{basis}}(i)$, which ranged from $-\pi/4$ to $\pi/4$, were selected in a symbol-by-symbol manner, as shown in Fig. 1(b). The angles were randomly generated using the seed key (typically 256 bits) and pseudorandom number generators (PRNGs). The procedure is detailed in [16]

After the random phase rotation, the constellation became a high-order PSK signal, as shown in Fig. 1(c). Provided that the resolution of the rotation angles was $\pi/2^{(m+1)}$ for $M = 4$, the order of PSK became $2^{(m+2)}$. The bit resolution m was set at a number as large as possible for higher secrecy. We could intuitively surmise that eavesdropping attempts to correctly detect the high-order PSK, e.g., 16,384 PSK for $m = 12$ and $M = 4$, were prevented by noise. On the other hand, a legitimate receiver who knew the angles of rotation for each symbol $\theta_{\text{basis}}(i)$ could detect the original QPSK signal by subtracting $\theta_{\text{basis}}(i)$ in a symbol-by-symbol manner. Provided that m was particularly large, adjacent signals were masked by quantum noise, as shown in the magnified image of Fig. 1(c). The quantum noise masking provided irreducible secrecy since quantum noise is truly random and is inherently inevitable at detection. The masking effect for secrecy is quantitatively discussed by defining a masking number Γ as the ratio of $\Delta\phi_{\text{shot}}$ and $\Delta\theta_{\text{basis}}$:

$$\Gamma = \frac{\Delta\varphi_{\text{shot}}}{\Delta\theta_{\text{basis}}} = \frac{M \cdot 2^m}{2\pi}\sqrt{\frac{2h\nu_0 B}{\eta_{\text{q}} P_0}}, \qquad (1)$$

where h, ν_0, B, η_{q}, and P_0 are Planck constant, signal frequency, signal bandwidth, quantum efficiency, and signal average power, respectively. The masking number indicates the number of signal phase levels covered by the variance of quantum noise. Here, the masking number is defined assuming an ideal heterodyne measurement, unlike our previous studies [9]–[11], [17] where an ideal phase measurement is assumed. The masking effect is proportional to the square root of the signal frequency ν_0 and is inversely proportional to the square root of the average power P_0. Typically, microwave frequencies are three to five orders of magnitude lower than optical ones while the average power required for transmission with error-free detection is similar. Hence, sufficient masking by quantum noise at microwave frequencies is difficult to achieve.

B. Photonic Generation of Cipher at Microwave Frequencies

Optical heterodyne was utilized to generate the cipher at microwave frequencies (<100 GHz). Fig. 2 shows the configuration for the conversion of the quantum noise masking from optical to microwave frequencies. First, the cipher was generated at an optical frequency f_{opt} ($\sim$ 200 THz) by a prescribed encryption protocol. As the frequency was high enough, sufficient masking by quantum noise was achieved here. Optical heterodyne was then employed to shift f_{opt} to a target microwave frequency f_{micro}. An LO light that had a frequency $f_{\text{opt}} + f_{\text{micro}}$ or $f_{\text{opt}} - f_{\text{micro}}$ was mixed with the cipher. Then, the cipher and LO were detected simultaneously by a photo detector (PD). The frequency of the cipher was shifted to the microwave difference

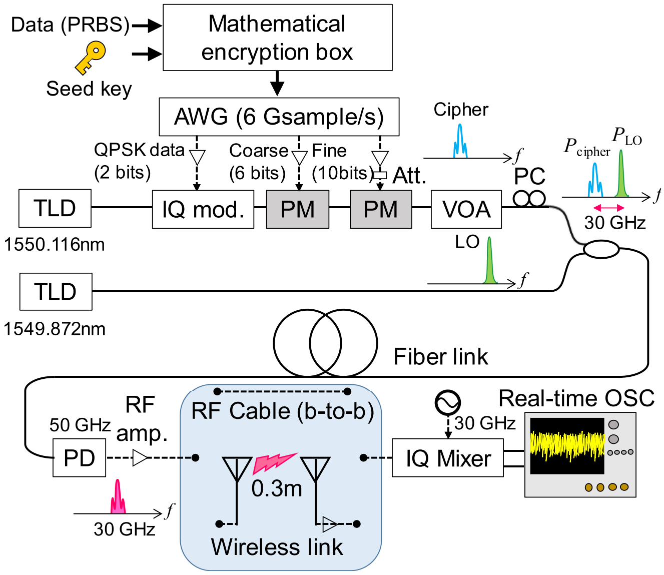

Fig. 3. Experimental setup of the coherent analog RoF cipher system utilizing quantum noise masking.

frequency f_{micro}. During this process, the quantum noise in the optical domain was added naturally and seamlessly to f_{micro}. Thus, the cipher with sufficient masking by quantum noise at f_{micro} was generated, and irreducible secrecy was achieved.

This microwave cipher system fit well with coherent analog RoF systems as the basic configuration using optical heterodyne with LO was consistent. In Fig. 2, the optical encryption and the antenna with optical heterodyne process are supposed to be in the base band unit and remote radio head, respectively. They were connected via a fiber cable as an optical fronthaul link, and the frequency shift was achieved near the antenna. While quantum noise is one of the fundamental limits on signal quality in analog RoF systems, it contributed to the secrecy in this cipher system. The biggest advantage here was that both the optical fronthaul and microwave wireless links could be simultaneously secured against interception. Thus, total physical layer security of the RoF system was achieved by the effect of the quantum noise masking. Although a single-channel system was considered here, this technique would be applicable to WDM systems in a multi-user scenario.

III. Experiments

A. Encryption and Decryption

We demonstrated a quantum noise-assisted 12 Gbit/s RoF cipher system based on QPSK data for 30 GHz wireless transmission. Fig. 3 shows the experimental setup. A data stream consisting of a pseudorandom binary sequence (PRBS) with a length of $2^{23}-1$ and a pre-shared seed key were put into a mathematical encryption box. Random phase rotation angles $\theta_{\mathrm{basis}}(i)$ were generated in the box. First, PRNGs extended the seed key to a key stream that was a very long PRBS. Here, the bit resolution of phase randomization m was set to 16, such that 16 bits of the key stream were consumed to generate one random angle. A mapper was used to determine the rotation angle $\theta_{\mathrm{basis}}(i)$ from the 16 bits of the key stream. Additionally, the polarity of the QPSK data was randomized according to the key stream. These process were implemented offline.

Three optical modulators were driven by the outputs from the box via a 6 Gsample/s arbitrary waveform generator. The coherent light at 1550.116 nm from a tunable laser diode was modulated by an IQ modulator with the polarity-randomized QPSK data (2 bits). Then, coarse-to-fine phase randomization using two cascaded phase modulators (PMs) [9] was employed for the phase randomization of the QPSK signal. The phase rotation angles with 16-bit resolution were divided into coarse (6-bit resolution) and fine (10-bit resolution) angles, and the two PMs were synchronously driven by them. The driving voltages were adjusted with radio frequency (RF) amplifiers and attenuators such that the coarse-to-fine relationship described in [11] was satisfied. Thus, the cipher with 2^{18} phase levels was generated at 1550.116 nm.

Next, the cipher was combined with an LO light at 1549.872 nm. The wavelength difference between the LO and cipher was approximately 30 GHz. As this experiment was a proof-of-concept demonstration, the wavelength difference was not precisely locked to 30 GHz. Precise locking is necessary for practical uses. The cipher and LO were transmitted over a fiber link and detected simultaneously by a PD with a 50 GHz bandwidth. This heterodyne process generated the cipher at a center frequency of 30 GHz while keeping sufficient masking by quantum noise. The cipher at 30 GHz was amplified and transmitted over a short RF cable for a back-to-back condition or a 0.3 m wireless link using a pair of horn antennas and an RF amplifier. The distance of the wireless link was limited by the size of the microwave shielding used. At the receiver, the cipher was down-converted with an IQ mixer and an LO at 30 GHz. An oscilloscope with 6 GHz analog bandwidth was used for digitization. Finally, digital signal processing (DSP) was performed offline. The DSP incorporated decryption of the cipher, which was a symbol-by-symbol subtraction of the angle of phase rotation. This process was performed before carrier phase recovery.

We demonstrated encryption and decryption in a back-to-back condition with a short RF cable. The output of the coupler was directly connected to the PD. The optical powers of the cipher P_{cipher} and LO P_{LO} at the coupler output were set to -9.0 and 6.3 dBm, respectively. Fig. 4(a) shows the optical spectrum at the input of the PD. The optical frequency difference between the cipher and LO was approximately 30 GHz. Fig. 4(b) shows the electrical spectrum after heterodyne detection. The cipher was successfully generated at the center frequency of approximately 30 GHz. We then measured constellations and Q values. Fig. 5(a) shows the constellations before and after the decryption. The QPSK constellations were successfully recovered, and bit errors were not observed for the measured 2^{20} bits. Fig. 5(b) shows Q values of the cipher after the decryption and the noncipher QPSK signal (reference). P_{cipher} changed from -9 to -23 dBm while P_{LO} was constant at 6.3 dBm. Q values of the cipher after the decryption were more than 16.5 dB. A large Q margin from a Q threshold of soft-decision forward error correction (SD-FEC) (7.3 dB) was achieved. The Q penalty from

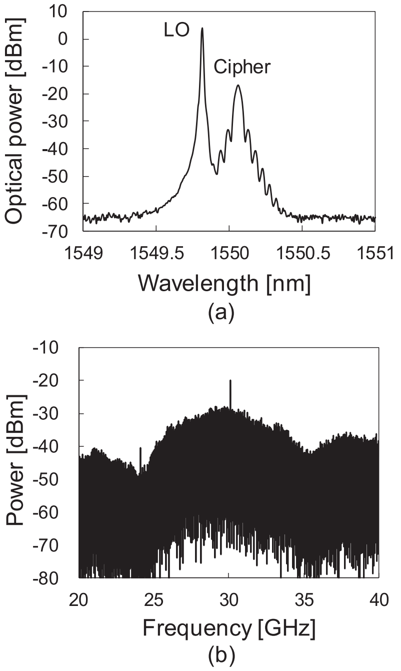

Fig. 4. (a) Optical spectrum at the input of the PD, and (b) Electrical spectrum after heterodyning.

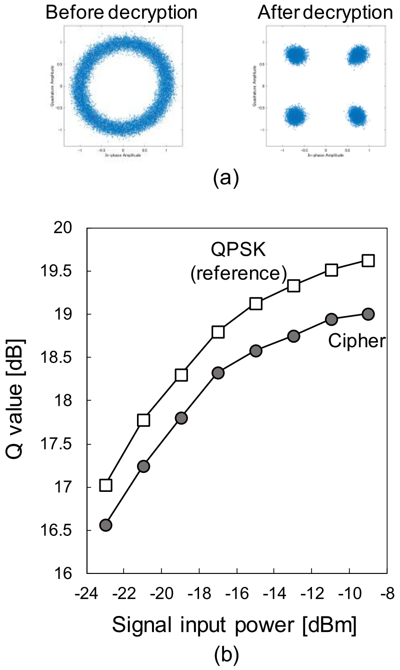

Fig. 5. Experimental results of the encryption and decryption in a back-to-back condition: (a) Constellation diagrams before and after decryption, and (b) Q values of the cipher and reference QPSK for various optical input powers.

the reference curve of the QPSK signal was, at most, 0.6 dB. Encryption and decryption were achieved without significant negative impacts on the signal quality.

B. Cipher Transmission Over Fiber and Wireless Links

We replaced the RF cable with the pair of antennas and demonstrated wireless transmission over the 0.3 m wireless link.

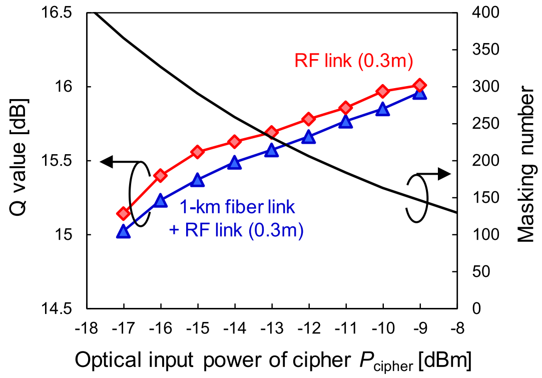

Fig. 6. Q values and the lowest quantum noise masking number in the fiber and wireless links when the optical input power of the cipher changed.

Fig. 6 shows Q values when P_{cipher} changed from -9 to -17 dBm. The red and blue curves indicate Q values without and with transmission over a 1 km fiber link, respectively. Q values were more than 15 dB after the fiber and wireless transmissions, and a Q margin of more than 7.5 dB from the SD-FEC threshold was achieved for measured P_{cipher}. In the current setup, the RF power of the cipher at the input of the antenna was limited to less than 0.5 mW by the gain of the RF amplifier we used. Larger Q margins for a practical lossy wireless link could be achieved with a higher gain amplifier. Furthermore, the use of an optical amplifier before the PD was beneficial in significantly enhancing the distance of the fiber link, although loss of a few dB was acceptable without it.

The black curve in Fig. 6 shows the quantum noise masking number calculated by substituting P_{cipher} into P_0 in Eq. (1) with $\eta_q = 1$. P_{cipher} is the optical power at the input of the fiber link and highest in this system. Since the masking number is inversely proportional to the square root of the optical power P_0, the masking number becomes lowest for P_{cipher}. In other words, tapping at the input of the fiber link is the best case for an eavesdropper. The curve indicates that the masking numbers were kept at more than 100, and even had the eavesdropper tapped all of the power of the cipher at the input. Thus, adequate signal quality and security based on the quantum noise masking were simultaneously achieved in this RoF cipher system.

IV. Security Consideration

Security of the RoF cipher system was ensured by the quantum noise masking. Here, the masking effect along the fiber and wireless links is discussed. Fig. 7 shows the schematic image of the change in the masking number along the fiber and wireless links. As mentioned in the previous section, the masking number at the input of the fiber link Γ_{input}, calculated by substituting P_{cipher} into P_0 in Eq. (1), was the lowest in this system. Along the fiber link, the masking number gradually increased as the power of the cipher decreased due to the fiber loss. When the total attenuation of the fiber links was α_{fiber}, received optical power at the PD was $P_{\text{PD}} = \alpha_{\text{fiber}} \cdot P_{\text{cipher}}$. The masking number in the wireless link Γ_{wireless} was calculated by substituting P_{PD} into

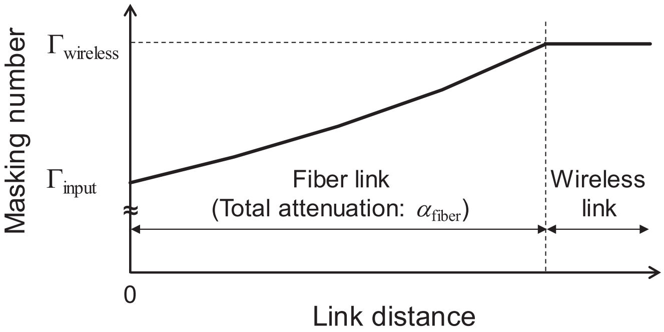

Fig. 7. Schematic diagram of the change in the quantum noise masking number along the fiber and wireless links.

P_0 in Eq. (1). Although the power of the cipher at microwave frequency decreased as it propagated, the masking number was virtually constant along the wireless link as the masking effect on the microwave carrier frequency was negligible.

Next, the meaning of the masking number for the practical security of the cipher system is discussed. Here, we focused on typical attacking on a seed key and/or data where an eavesdropper intercepts the extremely high-order signals of the cipher and subsequently analyzes them using computational resources. Discrimination of the phase levels was an essential first step as the subsequent analysis was effective for correctly measured levels. However, such discrimination was inevitably disrupted by the quantum noise masking. In the following, we consider the case of our experiments, in which the cipher was 2^{18}-levels PSK at 6 Gbaud. When an eavesdropper intercepted all of the power of the cipher at the input of the fiber link (the best case for an eavesdropper), the masking number followed the black curve seen in Fig. 6. As an example, masking of 146 phase levels ($\Gamma_{\text{input}} = 146$) was achieved at the maximum P_{cipher} of -9 dBm in the experiments. This meant that the probability of correctly pinning down a phase level was approximately 1/146, even if an eavesdropper without the seed key had used an ideal heterodyne receiver limited only by quantum noise. In practice, obtaining the correct phase levels of consecutive symbols is required to deduce a seed key and/or to decipher data messages. The probability of successful phase measurement of consecutive l symbols is approximately $(1/146)^l$. The symbol length l required to deduce a seed key by the subsequent analysis depends on the procedure in the mathematical encryption box. It is typically large, and the probability is very small in practice, e.g., 5.5×10^{-70} for $l = 32$. Detailed discussions of the practical security in the optical domain are provided in other studies [18]$-$[20]. Another interception point was the wireless link. The quantum noise masking number of the cipher at a center frequency of 30 GHz was 164 when P_{cipher} and α_{fiber} were -9 dBm and 0.8 (1 dB), respectively. The masking number was estimated to be slightly higher than this value in practice because the quantum efficiency η_{q}, which was assumed to be 1 here, was lower than 1. The probability of correctly pinning down the phase levels of consecutive l symbols without the key became 1.3×10^{-71} for $l = 32$ in the wireless link. Thus, high practical security was achieved both in the optical fronthaul and microwave wireless links.

V. Conclusion

We have experimentally demonstrated a proof-of-concept 12 Gbit/s coherent RoF cipher system using optical heterodyne frequency shift for secure optical fronthaul and 30 GHz-band wireless links. In the system, sufficient quantum noise masking of more than 100 was achieved for the ciphers, both at the optical and microwave frequencies. The Q penalty caused by the encryption and decryption was only 0.6 dB, which indicated that high security against interception from the physical layer can be achieved at small cost for transmission performances. The security can neither be modified nor breached by an eavesdropper as quantum noise with which signals are masked for encryption is truly random and is inevitable at signal detection. In the experiments, the wireless link distance was limited to 0.3 m because of the size of shielding. Transmission over a longer distance was feasible. Moreover, a larger Q margin for practical lossy wireless links could be achievable with a higher gain RF amplifier. The distinctive advantage of this RoF cipher system was that both the optical fronthaul and microwave wireless links were simultaneously secured against interception. In addition, this approach was applicable to all microwave frequencies by simply adjusting the wavelength difference between the cipher and LO lights. Applications in various mission-critical network systems requiring high information security are expected.

Acknowledgment

The authors would like to thank Prof. K. Kato of Tamagawa University for fruitful discussion.

References

[1] V. H. Poor and F. R. Schaefer, “Wireless physical layer security,” *Proc. Nat. 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. Int. Conf. Intell. Adv. Syst.*, 2007, pp. 484–488.

[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 Wireless Symp.*, 2009, Paper TU2P-28.

[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, Aug. 2010.

[6] G. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure communication using mesoscopic coherent states,” *Phys. Rev. Lett.*, vol. 90, 2003, Art. no. 227901.

[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, 2005, Art. no. 062326.

[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*, vol. 72, no, 2, 2005, Art. no. 022335.

[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. Opt. Fiber Commun. Conf.*, 2019, Paper Th1J.7.

[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 *et al.*, "10-Gb/s optical transceiver using the Yuen 2000 encryption protocol," *J. Lightw. Technol.*, vol. 28, no. 18, pp. 2714–2723, Sep. 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. Technol. Lett.*, vol. 30, no. 22, pp. 1987–1990, Nov. 2018.

[14] M. Nakazawa *et al.*, "QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution," *IEEE J. Quantum Electron.*, vol. 53, no. 4, Aug. 2017, Art. no. 8000316.

[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. OptoElectronics Commun. Conf. Australian Conf. Opt. Fibre Tech.*, 2014, Paper MO1A2.

[16] F. Futami *et al.*, "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] K. Tanizawa and F. Futami, "Photonic generation of quantum noise assisted cipher at microwave frequencies for secure wireless links," in *Proc. Opt. Fiber Commun. Conf.*, 2020, Paper M4A.3.

[18] O. Hirota, "Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol," *Phys. Rev. A*, vol. 76, no. 3, 2007, Art. no. 032307.

[19] 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 I," *Proc. SPIE*, vol. 10409, 2017, Art. no. 104090I.

[20] 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," *Proc. SPIE*, vol. 10771, 2018, Art. no. 1077114.

Ken Tanizawa (Member, IEEE) received the B.E., M.E., and Ph.D. degrees all in electronic engineering from the University of Tokyo, Tokyo, Japan, in 2004, 2006, and 2009, respectively.

From 2007 to 2009, he was a Research Fellow of the Japan Society for the Promotion of Science. He was with the National Institute of Advanced Industrial Science and Technology (AIST), Japan, from 2009 to 2017, where he was involved in the research on silicon photonics and optical signal processing. In 2017, he joined Tamagawa University. He is currently an Associate Professor in Quantum ICT Research Institute of the university. His recent research interest includes secure optical transmission systems and silicon photonics devices for communications and computing.

Prof. Tanizawa is a member of the Institute of Electronics, Information, and Communication Engineers of Japan.

Fumio Futami (Member, IEEE) received the B.S., M.S. and Ph.D. degrees all in electronic engineering from the University of Tokyo, Tokyo, Japan, in 1995, 1997 and 2000, respectively.

In 2000, he joined Fujitsu Laboratories Ltd., Kawasaki, Japan, where he was mainly engaged in the research and development of ultra-high speed optical transmission systems and ultra-fast all-optical signal processing for optical communication systems. In 2010, he moved to Tamagawa University, Tokyo, Japan and started the research and development of the cipher communication employing physical phenomena for achieving high secrecy and high communication performance. He was promoted to a Professor in 2014 and has been serving as a Steering Committee of CLEO PR since 2016 and as a Technical Program Committee of OFC since 2019.

Prof. Futami is a member of IEEE, OSA, SPIE, and IEICE.