European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

Microwave OFDM Quantum-Noise Randomized QAM Cipher Generation via Analog IFoF Transmission with a DML

Ken Tanizawa, Fumio Futami

Quantum ICT Research Institute, Tamagawa University, Japan, tanizawa@lab.tamagawa.ac.jp

Abstract *We demonstrate an IM/DD IFoF transmission system using a DML for the delivery and generation of 4.25-Gbit/s OFDM quantum-noise randomized QAM cipher at an IF of 1.875 GHz. The simplified setup achieves truly random quantum-noise signal masking for preventing interception while maintaining high signal quality. ©2022 The Author(s)*

Introduction

Security of wireless systems is increasingly important for future networks, e.g. 6G or beyond. Current systems use symmetric-key encryption algorithms in digital layers, such as the advanced encryption standard (AES), where security is based on computational complexity. While cryptanalysis of encrypted digital data is prevented with AES, illegitimate signal reception and demodulation are not prevented. To directly protect signals for high security, two approaches have been studied: physical layer security based on advanced coding [1] and physical layer encryption (PLE) utilising unique signal encoding and/or modulation with a private key [2–5].

Recently, photonic-assisted microwave PLE based on signal masking by quantum (shot) noise has been demonstrated for wireless systems [6]. Data (plaintext) is converted to optical extremely high-order signals utilising a prescribed protocol with a pre-shared seed key. Then, heterodyne frequency conversion from the optical to an intended microwave frequency is performed. Through the signal generation at an optical high frequency, the adjacent signals are sufficiently masked by quantum noise, which cannot be realized with direct microwave signal synthesis. The quantum-noise signal masking imposes true uncertainty on the encrypted microwave high-order signals and inevitably induces errors on illegitimate signal reception. Thus, irreducible signal security is achieved. This approach was applied to the microwave cipher generation via intensity-modulation/direct-detection (IM/DD) analog IF-over-fibre (IFoF) transmission. 4.09-Gbit/s orthogonal frequency-division multiplexing (OFDM) PSK-based encryption at an intermediate frequency (IF) was demonstrated [7], where optical coarse-to-fine modulation with a dual-electrode MZI [8] was employed to improve the resolution of the wideband modulation beyond a single digital-to-analog (D/A) converter.

This paper reports an IFoF transmission system with a directly modulated laser (DML) for simplified microwave OFDM quantum-noise randomized cipher generation. Because the coarse-to-fine modulation cannot be utilized with a DML, analog bandwidth of D/A conversion at Tx. is reduced to maintain a sufficiently high resolution. To mitigate the effect of the limited bandwidth, we employ quadrature amplitude modulation (QAM)-based encryption with 16QAM data modulation. Analog IFoF transmission with a DML over a 10-km fibre link is demonstrated with a negligibly low penalty. 4.25-Gbit/s line rate OFDM QAM-based cipher at an IF of 1.875 GHz is generated. More than 50 adjacent encrypted QAM signals are masked by quantum noise for secrecy, and a symbol error ratio (SER) an eavesdropper could reach is limited higher than 0.99. The error vector magnitude (EVM) after the transmission and decryption is approximately 3 % at an optical received power of 2 dBm, which is comparable with that of reference non-cipher 16QAM. The cipher system effectively prevents microwave signal interception while maintaining high signal quality. The effect of additive noises on the signal security is also discussed.

Operating principles and system design

Fig. 1 shows the operating principle of the signal encryption based on quantum-noise masking via analog IM/DD IFoF transmission. Data (plaintext) and a pre-shared private seed key are placed in the mathematical encryption box. Here, QAM-based encryption is employed. Amplitude biases are added to the in-phase and quadrature (IQ) components of the low-order QAM data-modulated signals (16QAM in the figure). The amount of bias is determined using pseudorandom number generators (PRNGs) and seed key in a symbol-by-symbol manner. Thus, the encrypted signals correspond to an extremely high-order QAM template with an order of 2^{20} or higher. Next, OFDM modulation is performed, followed by frequency up-conversion to an IF of f_{IF}. Then, optical intensity is modulated by the electrical IF signals. A DML is used in the following experiments. After transmission over a fibre link, the optical signals are detected with a

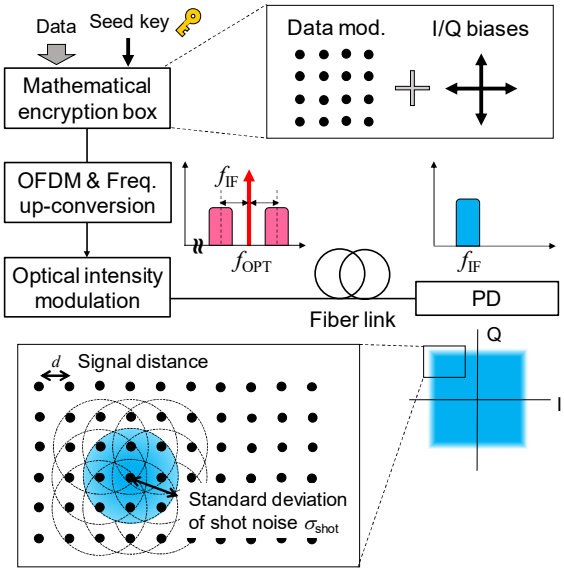

Fig. 1: Operating principle of QAM-based encryption with quantum-noise masking via IM/DD IFoF transmission.

photodetector (PD), and quantum noise is added to the IF signals. The order of QAM after the encryption is high, such that adjacent signals are masked by quantum noise, as shown in the magnified image of Fig. 1. Sufficient quantum-noise masking for signal security is achieved via photo-detection at a high optical carrier frequency f_{OPT} of typically 193 THz. Hence, error-free measurement of the encrypted signals by an eavesdropper without the private seed key is inherently prohibited. A legitimate receiver with the same PRNGs and private seed key can subtract the amplitude biases from the received IQ components. The effect of quantum noise on the decrypted low-order data-modulated signals is sufficiently small for error-free reception.

Quantum noise is truly random and unavoidable. Hence, the lower bound of signal security is promised by the quantum-noise signal masking. A quantum-noise masking number defined as the number of signals covered by quantum noise, is a typical security measure. A higher number means high security because uncertainty imposed on illegitimate signal reception is large. The masking number for QAM-based encryption $\Gamma_{\text{Q-qam}}$ is given by

$$\Gamma_{\text{Q-qam}} = \pi \frac{\sigma_{\text{shot}}^2}{d^2}, \qquad (1)$$

where σ_{shot} and d are the standard deviation of shot noise and signal distance of encrypted QAM signals, respectively, as shown in Fig. 1. We calculated $\Gamma_{\text{Q-qam}}$ for various optical modulation indexes (OMIs) in the IM/DD OFDM encryption system. Fig. 2 shows the results when the received power and signal bandwidth are 2 dBm and 1.25 GHz, respectively. A lower OMI achieves a higher masking number or higher security but reduces signal quality. The tradeoff is mitigated by increasing the order of encrypted QAM signals. We use a 2^{24} QAM template to realize $\Gamma_{\text{Q-qam}} > 50$ in the following experiments.

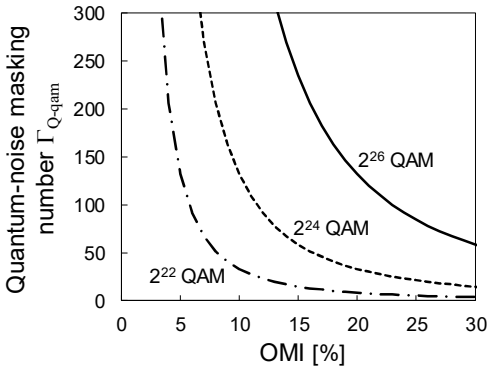

Fig. 2: Quantum-noise masking number for various OMIs at P_{rec} = 2 dBm.

Experiments

We demonstrated OFDM quantum-noise randomized QAM cipher generation at an IF of 1.875 GHz via IM/DD analog transmission. Fig. 3 shows the experimental setup. We assume here that a private seed key of 256 bits is preliminarily shared between the transmitter and receiver. Data consisting of PRBS (plaintext) is converted to OFDM extremely high-order QAM signals at an offline digital signal processing (DSP) part with the seed key. The flow of DSP basically follows our previous work of PSK-based encryption with QPSK data modulation [7]. Here, QAM-based encryption is employed. The data bits are sliced every four bits for 16QAM data modulation. Meanwhile, random 20 bits are generated using the seed key and PRNGs. They are added to each four data bits, generating encrypted signals on a 2^{24} QAM template. Subsequently, OFDM modulation with signal bandwidth of 1.25 GHz and 128 subcarriers is performed. The bit rate excluding the cyclic prefix and preamble for OFDM is 4.25 Gbit/s. Finally, the frequency is up-converted to an IF of 1.875 GHz. An arbitrary waveform generator (AWG) with 10 Gsample/s and 16-bit nominal resolution [9] is used for D/A

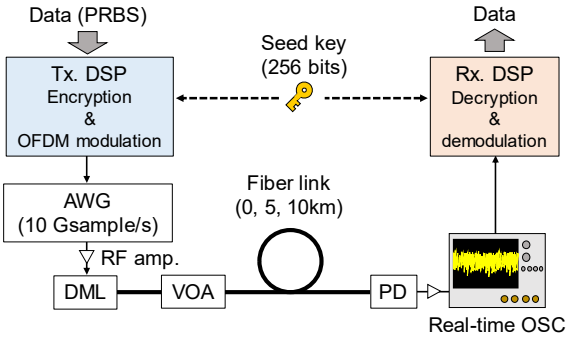

Fig. 3: Experimental setup.

conversion. A DML operating at 1550 nm is driven by the AWG output. The optical IM signals are transmitted over a fibre link and detected with a PD. Quantum noise is added upon detection, and OFDM quantum-noise randomized QAM signals are generated at 1.875 GHz. Here, we evaluate the signals using offline DSP with down conversion, OFDM demodulation, and decryption.

First, signal quality in an optical back-to-back condition was investigated. Figs. 4(a) and (b) show the electrical spectrum and constellation diagrams before and after the decryption when received power P_{rec} and OMI were 2 dBm and 10.7 %, respectively. The encrypted signals were generated at a centre frequency of 1.875 GHz. The constellation diagram before decryption shows that extremely high-order QAM encrypted signals are successfully generated. Correct signal discrimination is prevented by noises. After the decryption with a private seed key, 16QAM data-modulated signals were recovered. Fig. 5 shows the EVMs of decrypted and reference 16QAM signals for different OMIs at a received power P_{rec} of 2 dBm. Lower EVMs are achievable for higher OMIs, whereas signal security decreases as OMI increases, as shown in Fig. 2. To balance the signal quality and security, we set OMI to 12 % in the following experiments.

Fig. 6 shows EVMs (red and blue curves) and the lower bound of SER for an eavesdropper (black one) for various received powers after transmission over 0 (B-to-B), 5, and 10 km. The red and blue curves indicate the results of decrypted and reference non-cipher 16QAM signals, respectively. The EVM after decryption was approximately 3.8 % at P_{rec} = 0 dBm. The penalty caused by the encrypted transmission was less than 0.8 % in the measured power range, which was sufficiently low in practice. The black curve shows SER estimated from the quantum-noise masking number $\Gamma_{\text{Q-qam}}$. This value is the lower bound that an eavesdropper without a private seed key could achieve only if quantum noise is present. The SER was higher than 0.99 for $P_{rec} \leq 4$ dBm and sufficiently high for preventing signal interception.

The effect of additive noises on the signal masking is discussed. The effective number of bits of the AWG used was approximately 10 at 1 GHz. The clipping ratio was 13 dB. We estimated the noise from D/A conversion, sum of clipping and quantization noises, based on the analysis shown in [10]. The noise from D/A conversion was approximately an order of magnitude smaller than quantum noise at P_{rec} = 0 dBm. The relative intensity noise (RIN) of the DML used was typically −155 dB/Hz at 1 GHz, which indicates that RIN was comparable with quantum noise at P_{rec} = 0 dBm. These additive noises enhance the signal security in practice as long as they can be considered as random. Nevertheless, quantum noise is particularly important because the true randomness contributes to proven signal security which can never be reduced by any means.

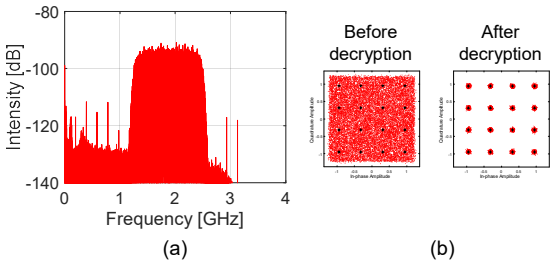

Fig. 4: (a) Electrical spectrum and (b) constellation diagrams before and after decryption.

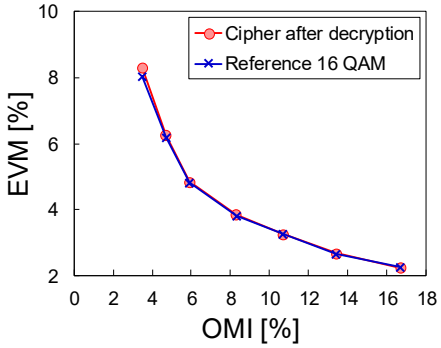

Fig. 5: EVM for different OMIs at P_{rec} = 2 dBm.

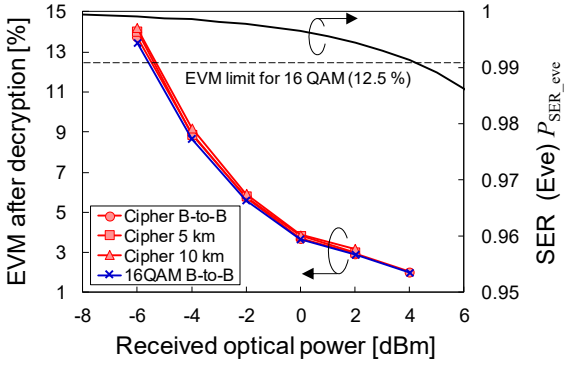

Fig. 6: EVM after decryption and SER for an eavesdropper in IFoF transmission over 0, 5, and 10 km fibre.

Conclusions

We have demonstrated a simple analog IFoF transmission system with a DML for the delivery and generation of 4.25-Gbit/s OFDM quantum-noise randomized QAM cipher at IF of 1.875 GHz. Truly random signal masking by quantum noise for irreducible security against interception was achieved while maintaining high signal quality.

Acknowledgements

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. DOI: doi.org/10.1073/pnas.1618130114

[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. DOI: 10.1109/ICIAS.2007.4658435

[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. DOI: 10.1364/OE.26.022296

[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. DOI: 10.1109/RWS.2009.4957350

[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. DOI: 10.1109/TCE.2010.5606266

[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. DOI: 10.1109/JLT.2020.2987213

[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. DOI: 10.1109/JLT.2021.3119603.

[8] K. Tanizawa, and F. Futami, "2^{14} Intensity-Level 10-Gbaud Y-00 Quantum Stream Cipher Enabled by Coarse-to-Fine Modulation," IEEE Photonics Technology Letters, vol. 30, no. 22, pp. 1987-1990, 2018. DOI: 10.1109/LPT.2018.2874236

[9] https://www.tek.com/arbitrary-waveform-generator/awg5200

[10] E. Vanin, "Performance evaluation of intensity modulated optical OFDM system with digital baseband distortion," Opt. Express vol. 19, no. 5, pp. 4280-4293, 2011. DOI: 10.1364/OE.19.004280