Secure Free-Space Optical Transmission of IM and PSK Y-00 Quantum Stream Cipher under Dense Fog Conditions

Fumio Futami[(1)], and Ken Tanizawa[(1)]

[(1)] Quantum ICT Institute, Tamagawa University, Japan, futami@lab.tamagawa.ac.jp

Abstract *We demonstrate free-space Y-00 cipher transmission in artificial dense fog with a high attenuation of 20 dB. The Y-00 cipher carrying 1.5 Gb/s IM and 10 Gb/s DP BPSK signals are securely transmitted in such a harsh condition where the FSO receiver is invisible from the transmitter. ©2023 The Author(s)*

Introduction

Free space optics (FSO) communication is a type of optical communication that utilizes light propagation through free space, offering high bandwidth and capacity [1,2]. With the current overcrowding of bandwidth in wireless communication systems that exploit radio frequency, FSO communication has become an attractive solution for next-generation wireless communications [3]. However, FSO communication is subject to atmospheric effects, and its propagation characteristics in free space are influenced by weather conditions, such as clouds, snow, fog, rain, and turbulence, which can cause excessive losses. To investigate such effects, hardware simulators are used, as waiting for natural phenomena to occur can be inefficient. For instance, an optical turbulence generator can simulate atmospheric turbulence [4]. Among the various atmospheric effects, fog causes significant transmission loss, which limits the transmission distance. Therefore, researchers have investigated transmission characteristics in fog to derive an empirical model for fog attenuation prediction [5,6].

Another feature of FSO communication is its high security owing to the high directivity of the laser beam. However, the data may be compromised by tapping the signal in free space. To address the issue of signal tapping, Y-00 cipher employing multilevel optical modulation techniques is promising because it enhances security and protect against signal interception [7,8]. Figure 1 illustrates the encryption and decryption principle of binary phase-shift keying (BPSK) signals as an example. BPSK signals are converted into ultra-dense multilevel signals using an encryption key in the transmitter. The legitimate receiver with the key decrypts the ultra-dense multilevel cipher signals to recover the original binary data in the receiver. In contrast, an eavesdropper (Eve) without the key cannot accurately identify the cipher signal due to noise, which ultimately comprises quantum noise that masks the cipher signal. Notably, the Y-00 cipher has been successfully applied to FSO communication in conditions with no atmospheric effects [9].

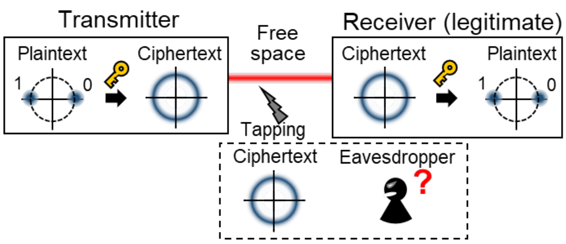

Fig. 1: Concept of the Y-00 cipher in which a cipher signal is masked by quantum noise and protected from eavesdropping.

In this study, we investigated the transmission of the Y-00 cipher via free-space optics under artificially generated dense fog conditions. Specifically, we transmitted 1.5 Gb/s intensity-modulated (IM) Y-00 cipher and 10 Gb/s dual-polarization (DP) PSK Y-00 cipher over a distance of 108 cm in a fog chamber. Despite severe visibility limitations and a high attenuation of 20 dB, we were able to achieve successful cipher communication. Furthermore, our results indicated that the transmission was highly secure, as evidenced by Eve's symbol error rates (SERs).

Experimental Setup

Figure 2 presents a schematic of the setup used in the Y-00 cipher transmission experiments, which included the free-space transmission within a fog chamber. We applied two modulation formats for the Y-00 cipher signals in

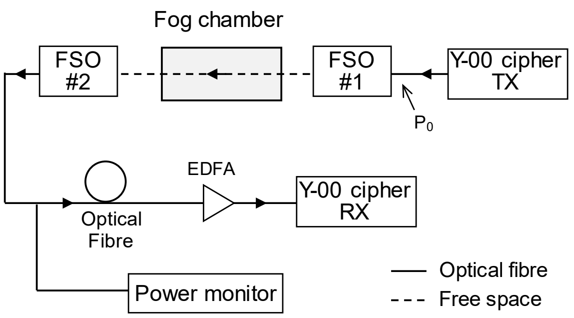

Fig. 2: Schematic of the experimental setup for Y-00 cipher communication under dense fog conditions.

this study. The first was intensity modulation at a data rate of 1.5 Gb/s with intensity levels of 2^{12} (= 4,096), prepared by a real-time Y-00 cipher transceiver [10] at a wavelength of λ_S = 1550.1 nm. The other was 10-Gb/s DP PSK at λ_S = 1550.1 nm with phase levels of 2^{16} (= 65,536). Binary data were encrypted using a 256-bit common key to generate multilevel cipher signals in the Y-00 cipher transmitter (TX). The cipher signals in an optical fibre were transmitted to free space through FSO #1. A laser beam carrying the cipher signals was directed through a laser window hole on the right side of a fog chamber [11]. The laser beam had a diameter of 12 mm. Further details regarding FSO can be found in [12]. Figure 3 shows a photo of fog chamber. The chamber width, which corresponded to the transmission distance of the laser beam in the fog, was L_0 = 108 cm. The depth and height were 45 and 35 cm, respectively. Letters ("Tamagawa") and a small doll displayed at the back of the chamber are visible. To achieve a uniform fog density, we inputted artificial fog generated by an ultrasonic atomizer (Honda Electronics Co. Ltd., Ultrasonic atomizer unit JM-200) from a fog window hole on the top of the chamber. The inflow amount of fog was kept constant throughout the experiment. The particle size of the fog generated by the atomizer was approximately 3 μm, which is slightly smaller than that of natural fog. The laser beam was output from a laser window hole on the left side of the fog chamber and coupled into an optical fibre through FSO #2. The signal power loss from the fibre input of FSO #1 to the fibre output of FSO #2 was measured to be 8.7 dB without the presence of fog. The excess loss was monitored every 5 s using an optical power meter at the output end of FSO #2, using the average mode.

An optical fibre with a length of 25 km and loss of 5 dB was used after FSO #2 to demonstrate transparent conversion of the cipher signals from free space into an optical fibre for further transmission. The cipher signal was then preamplified and decrypted in a Y-00 cipher receiver (RX) using a 256-bit common key shared with the transmitter. The bit error rate (BER) was measured in real time for the 1.5 Gb/s IM Y-00 cipher signals. As for the 10-Gb/s DP PSK Y-00 cipher signal, it was received by an intradyne coherent receiver, and then subjected to offline digital signal processing for decrypting the cipher signals and calculating the Q-values.

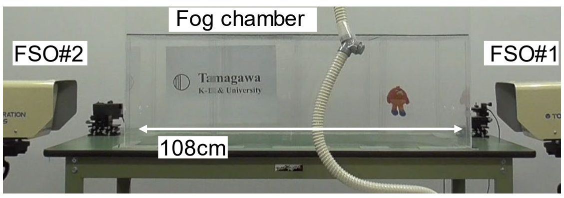

Fig. 3: Image of a fog chamber with no excess loss, FSO #1 and FSO #2.

The measurements were conducted by gradually increasing the fog density from a fog-free state. Once the excess loss due to fog reached 20 dB, the inflow of fog was stopped. The measurements were continued until the excess loss caused by fog was eliminated.

Results and Discussion

Initially, a 1.5 Gb/s IM Y-00 cipher was transmitted, with the optical power of the Y-00 cipher signal in FSO #1 set to P_0 = 0 or -6 dBm. Figure 4 depicts the excess losses caused by the fog chamber. The excess losses reach 20 dB after approximately 10 min of activating the fog generator. Then, after turning off the fog generator, the fog clears in approximately 7 min. Figure 5 shows a photo of the fog chamber when the excess loss reaches 20 dB. The fog appears uniform. The letters and doll displayed at the back of the chamber, which are beyond the 45-cm (the chamber depth) thick fog, are not clearly visible. In the receiver, the shared key was used to decrypt the multilevel cipher signal and recover a binary signal. The waveforms before and after decryption are shown in the inset of Fig. 6. The BERs of the decrypted binary signals were measured every 5 s to observe the impact of the fog. Figure 6 demonstrates that the cipher communication remains functional (BER < forward error

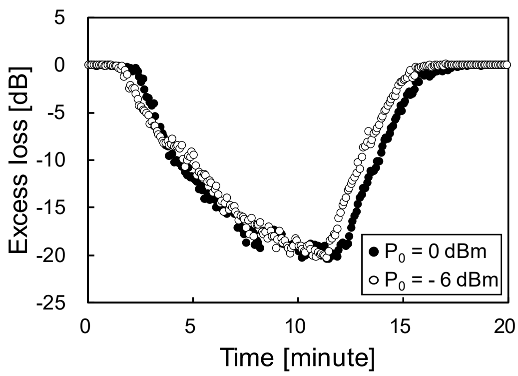

Fig. 4: Excess loss generated by artificial fog in the fog chamber for the 1.5-Gb/s IM Y-00 cipher.

Fig. 5: Image of a fog chamber with an excess loss of 20 dB and dense fog.

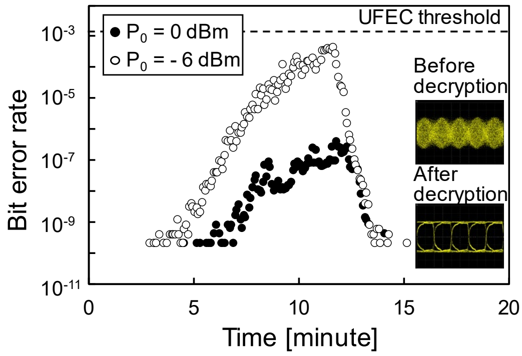

Fig. 6: BER of 1.5 Gb/s IM Y-00 cipher.

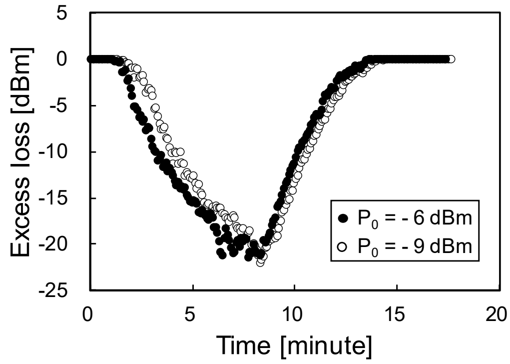

Fig. 7: Excess loss generated by artificial fog in the fog chamber for 10-Gb/s DP PSK Y-00 cipher signals.

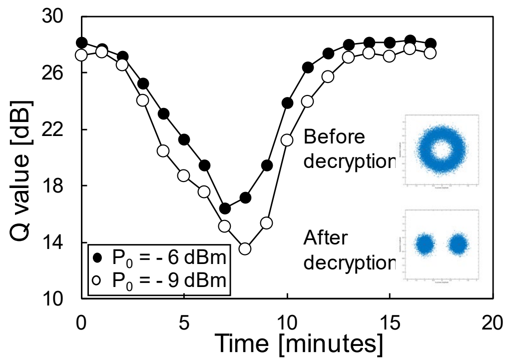

Fig. 8: Q values of 10-Gb/s DP PSK Y-00 cipher.

correction (FEC) limit) even at 20-dB excess loss for both P_0 values of 0 and -6 dBm. The fluctuations in the BERs are caused by minor variations in the excess loss. The absence of measurement results in the figure implies that no errors occurred. The security assessment of the system can be evaluated by considering the lowest SER of the Eve, which assumes that all signal power is tapped. It approaches 1 when signal discrimination completely fails, indicating a high level of security [13]. For P_0 = 0 dBm, the lowest SER of Eve is estimated to be 0.94, whereas for P_0 = -6 dBm, the lowest SER is 0.97. The security level is higher for P_0 = -6 dBm because lower power provides greater security in Y-00 cipher systems [13, 14]. In both cases, the cipher signals are effectively protected from signal interception because SER of 0.9 means 90 % of the tapped signals are incorrect for Eve.

Next, the 10-Gb/s DP BPSK Y-00 cipher was transmitted with P_0 = -6 or -9 dBm. The excess loss due to fog is shown in Fig. 7, which has similar characteristics to the previous IM Y-00 cipher experiments, except for faster fog thickening due to higher humidity in the chamber during measurement. Data was stored every minute, and Q values were calculated from the decrypted data. Figure 8 shows the Q values, with constellations before and after decryption shown in the insets. As the fog density increases, the Q values decreases, reaching 13.5 dB for P_0 = -9 dBm and 16.4 dB for P_0 = -6 dBm at the maximum excess loss. Assuming decrypted signals have Gaussian noise distribution, this achieves a BER < 10^{-9}, which is considerably lower than a typical FEC threshold, demonstrating that cipher communication is possible even in denser fog. The SER of Eve for P_0 = -9 and -6 dBm is 0.99 and 0.98, respectively, indicating that the FSO cipher communication system provides high security.

Even with an excess loss of 20 dB, FSO #2 was not visible from FSO #1. Nevertheless, secure communication was achieved. The visibility defined by the Kim model [15] was calculated as L_V = 70 cm when the excess loss was 20 dB. The transmission distance L_0 in the fog is 1.5 times longer than L_V, indicating that in natural fog with a visibility of 100 m, outdoor Y-00 cipher communication over 150 m is achievable. The use of higher optical power allows for an extended transmission distance. However, the security of the Y-00 cipher decreases in a high optical power regime. Typically, when using high optical power (>10 mW) for Gb/s data rate, a randomization technique called quantum deliberate signal randomization (QDSR) [16] is required to maintain high security.

Conclusions

FSO communication using Y-00 cipher was demonstrated in artificially generated dense fog with a high attenuation of 20 dB. It was shown both 1.5 Gb/s IM Y-00 cipher signals and 10-Gb/s DP PSK Y-00 cipher signals were securely transmitted over a 108-cm fog channel within the chamber.

Acknowledgements

The authors would like to acknowledge G. Masada for his help in constructing the fog chamber and TOYO Electric Corporation for the loan of the free-space optical communication system.

References

[1] K. Matsuda et al., "Demonstration of a Real-Time 14 Tb/s Multi-Aperture Transmit Single-Aperture Receive FSO System With Class 1 Eye-Safe Transmit Intensity," in Journal of Lightwave Technology, vol. 40, no. 5, pp. 1494-1501, 2022, DOI:10.1109/JLT.2021.3132306.

[2] F. P. Guiomar, M. A. Fernandes, J. L. Nascimento, V. Rodrigues and P. P. Monteiro, "Coherent Free-Space Optical Communications: Opportunities and Challenges," in Journal of Lightwave Technology, vol. 40, no. 10, pp. 3173-3186, 2022, DOI:10.1109/JLT.2022.3164736.

[3] M. Z. Chowdhury, M. Shahjalal, S. Ahmed and Y. M. Jang, "6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," in IEEE Open Journal of the Communications Society, vol. 1, pp. 957-975, 2020, DOI:10.1109/OJCOMS.2020.3010270.

[4] Vincent van Vliet, Menno van den Hout, Sjoerd van der Heide, and Chigo Okonkwo, “Experimental Investigation of Mode Diversity Reception Using an Optical Turbulence Generator and Digital Holography,” in European Conference on Optical Communication (ECOC) 2022, paper We5.56, 2022.

[5] M. A. Esmail, H. Fathallah, M, Alouin, “Outdoor FSO Communications Under Fog: Attenuation Modeling and Performance Evaluation,” IEEE Photonics Journal, Vol.8, 7905622, August 2016. DOI:10.1109/JPHOT.2016.2592705

[6] A. N. Khan, S. Saeed, Y. Naeem, M. Zubair, Y. Massoud and U. Younis, "Atmospheric Turbulence and Fog Attenuation Effects in Controlled Environment FSO Communication Links," in IEEE Photonics Technology Letters, vol. 34, no. 24, pp. 1341-1344, 15 Dec.15, 2022, DOI:10.1109/LPT.2022.3217072.

[7] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure Communication Using Mesoscopic Coherent States,” Phys. Rev. Lett. 90, 227901, 2003. DOI:10.1103/PhysRevLett.90.227901

[8] O. Hirota, M. Sohma, M. Fuse, and K. Kato, “Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme,” Phys. Rev. A 72, 022335, 2005. DOI:10.1103/PhysRevA.72.022335

[9] 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 14th Pacific Rim Conference on Lasers and Electro-Optics (CLEO PR 2020), paper C3F_4.m, 2020, DOI:10.1364/CLEOPR.2020.C3F_4

[10] F. Futami, K. Kato, and O. Hirota “A novel transceiver of the Y-00 quantum stream cipher with the randomization technique for optical communication with higher security performance,” Proc. SPIE 9980, Quantum Communications and Quantum Imaging XIV, 99800O, 2016 DOI:10.1117/12.2237852

[11] G. Masada, “Investigation of propagation characteristics of laser light and squeezed light in fog,” Proc. SPIE 12238, Quantum Communications and Quantum Imaging XX, 1223804, 2022, DOI:10.1117/12.2633384

[12] A. Bekkali, H. Fujita and M. Hattori, "New Generation Free-Space Optical Communication Systems With Advanced Optical Beam Stabilizer," in Journal of Lightwave Technology, vol. 40, no. 5, pp. 1509-1518, 2022, DOI:10.1109/JLT.2022.3146252

[13] K. Tanizawa and F. Futami, “Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system,” Opt. Express 29, 10451-10464, 2021, DOI:10.1364/OE.418302

[14] F. Futami, K. Tanizawa and K. Kato, "Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications," in Journal of Lightwave Technology, vol. 38, no. 10, pp. 2774-2781, 2020, DOI:10.1109/JLT.2020.2985709.

[15] I. I. Kim and E. J. Korevaar "Availability of free-space optics (FSO) and hybrid FSO/RF systems", Proc. SPIE 4530, Optical Wireless Communications IV, 2001. DOI:10.1117/12.449800

[16] F. Futami, K. Tanizawa, K. Kato, Y. Kawaguchi, and S. Sato, “Secure Unrepeated Fiber Transmission with Quantum Deliberate Signal Randomization on Y-00 Protocol,” in Optical Fiber Communication Conference (OFC) 2023, paper M2I.6, 2023.