Secure FSO Transmission with Quantum Deliberate Signal Randomization on the Y-00 Protocol under Fog Conditions

Fumio Futami[1*], Ken Tanizawa[1], Kentaro Kato[1], Yuichiro Hara[2], Michikazu Hattori[2], Abdelmoula Bekkali[2], and Yukihiko Suga[2]

[1] *Quantum ICT Research Institute, Tamagawa University, 6-1-1 Tamagawa-gakuen, Machida, Tokyo, 194-8610, Japan*
[2] *TOYO Electric Corporation, 2-156 Ajiyoshi, Kasugai, Aichi, 486-8585 Japan*
**futami@lab.tamagawa.ac.jp*

Abstract: Security-enhanced 10Gbit/s DP PSK Y-00 cipher transmission is demonstrated with deliberate signal randomization driven by quantum random number generator in free space in dense fog. High security and transmission performance are achieved over the entire transmission system. © 2024 The Author(s)

1. Introduction

Optical communication through free-space optics (FSO), providing high bandwidth and capacity [1,2], has become an attractive solution for next-generation wireless communications, as the radio-frequency bandwidth is frequently congested in wireless communication systems [3]. An advantage of FSO communication is the high level of security provided, which is due to the high directionality of the laser beam. However, data can be compromised if the signal is tapped in free space. Y-00 cipher utilizing multilevel optical modulation for signal-level encryption is a promising technology that protects optical signals from interception [4-6]. Figure 1(a) illustrates the principles of encryption and decryption for binary phase-shift keying (BPSK) signals. BPSK signals are converted into ultradense multilevel signals via an encryption key in the transmitter. The legitimate receiver with the key decrypts the ultradense multilevel cipher signals to recover the original BPSK signals. In contrast, an eavesdropper (Eve) without the key, cannot accurately identify the multilevel cipher signal because of noise, which ultimately consists of quantum noise that masks the cipher signal. The Y-00 cipher has been applied to FSO communication and has been demonstrated in an artificial dense fog channel with an additional loss of 20 dB [7]. In an FSO system, a higher power input is preferred to maintain a high signal-to-noise ratio. However, increasing the power decreases the security in a Y-00 cipher system. Figure 1(b) depicts an encrypted phase-shift keying (PSK) signal. Four neighboring signals are masked by quantum noise, preventing true signal discrimination. The number of signals masked by quantum noise, i.e., the noise masking number Γ_0, is used as a security measure. A higher noise masking number provides greater security. Γ_0 is proportional to $1/\sqrt{P_0}$, where P_0 is the optical power [8]. Thus, as shown in Fig. 1(c), the masking number or security of FSO transmission systems decreases in a high optical power regime, which is particularly required under harsh channel conditions such as a foggy atmosphere.

Here, we demonstrate a security-enhanced Y-00 cipher system with quantum deliberate signal randomization (QDSR) for FSO transmission under artificially created dense fog conditions. QDSR performs additive randomization of Y-00 cipher signals, using truly random numbers (TRNs) generated from a quantum random number generator (QRNG), and substantially enhances noise masking. Thus far, QDSR has been demonstrated only in optical fiber communication systems [9]. We successfully transmitted a 10 Gb/s dual-polarization (DP) PSK Y-00 cipher with QDSR over 108 cm in a fog chamber of severely limited visibility, followed by transmission through 25 km of single-mode fiber (SMF). Despite the use of a high input power of 0 dBm for a high link budget in FSO transmission, Eve's symbol error rates (SERs), estimated from the masking number, closely approach 1 throughout the entire link, indicating that the security is highly enhanced compared with the system without QDSR.

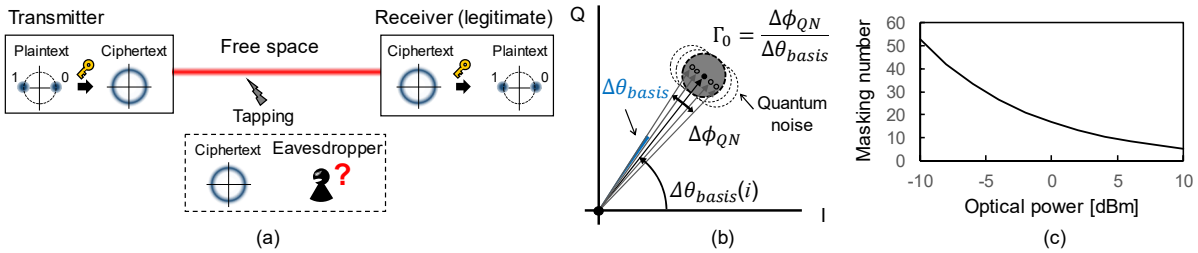

Fig. 1. (a) Concept of a Y-00 cipher system in which a cipher signal is masked by quantum noise and is protected from eavesdropping. (b) Illustration of masking by quantum noise. (c) A plot showing the masking number vs. optical power.

2. Noise Masking of Y-00 cipher with QDSR

The transmitter and receiver share a short key and mathematical encryption box in a Y-00 cipher system. QDSR, a DSR [10,11] driven by a QRNG, is installed in the transmitter and adds true randomness to cipher signals. Figure 2(a) illustrates a PSK Y-00 cipher signal with QDSR. A truly random phase rotation, $\theta_{QDSR}(i)$, determined by TRNs from a QRNG, is added to the phase rotation, $\Delta\theta_{basis}(i)$, in a bit-by-bit manner, based on the Y-00 protocol. The phase of each signal is rotated by $\theta_{basis}(i) + \theta_{QDSR}(i)$. The range of the QDSR phase rotation for the BPSK-based Y-00 cipher is $\pi\cdot\gamma_{QDSR}$, where the QDSR index, γ_{QDSR} ($0 \le \gamma_{QDSR} \le 1$), indicates the randomization depth. The level of uncertainty with QDSR exceeds that caused by the quantum noise, represented by a dotted circle in the figure; this leads to an increase in security. A legitimate receiver holding the preshared key can detect the original BPSK signal by subtracting $\theta_{basis}(i)$ in a bit-by-bit manner. Signal overlapping or uncertainty remains, even for a legitimate receiver, because TRNs for the QDSR are not shared between the transmitter and receiver. Hence, QDSR reduces the signal quality while enhancing security. Figure 2(b) shows the relation between masking number Γ_0 and optical power P_0 for 5 Gb/s BPSK-based Y-00 cipher signals with (dotted line) and without (solid line) QDSR. The phase levels after the encryption and the QDSR index γ_{QDSR} are 2^{16} and 0.2, respectively. The masking number with QDSR is expressed as $\Gamma_{QDSR} = (\Delta\phi_{QN} + \pi\cdot\gamma_{QDSR})/\Delta\theta_{basis}$ [9]. Γ_{QDSR} can be significantly higher, compared with those without QDRS, and almost independent of the optical power. Thus, QDSR enhances security even at high optical power. It should be noted that the power can be increased, as long as there is masking by quantum noise, as QDSR does not increase the quantum noise. Rather, it manipulates the phase of the signals by using TRNs from a QRNG, resulting in truly random phase fluctuation, which enhances security. Figure 2(c) shows the masking numbers with and without QDSR along a free-space link at an input optical power P_0 of 0 dBm. The horizontal axis indicates the loss caused by free-space transmission, corresponding to the distance of the link. In the case without QDSR (dotted line), the masking number is very small just after the transmitter where the additional loss is 0 dB. This suggests that the security is weak at the input of the link. However, QDSR significantly increases the masking number even at the input of the link, and high security is achieved all along the free-space link.

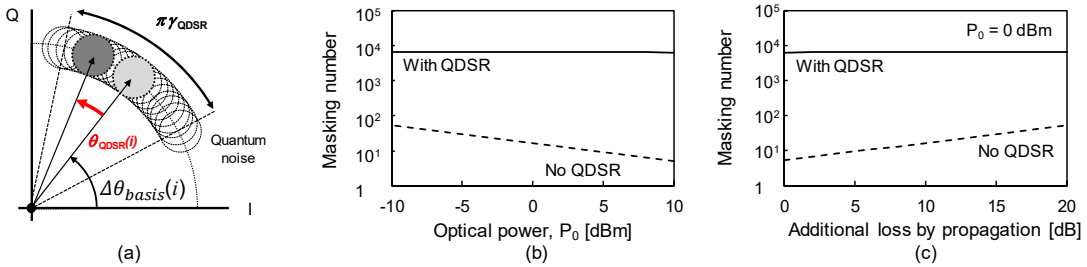

Fig. 2. (a) Illustration of making by QDSR. (b) Masking number at the transmitter end for 5 Gb/s BPSK signals with phase levels of 2^{16}, and (c) masking numbers with additional loss by free-space propagation.

3. Experiment

Figure 3 shows the experimental setup of the FSO transmission of a Y-00 cipher signal with QDSR under fog conditions. In the transmitter, the binary data were encrypted using a 256-bit common key to generate 5 Gb/s PSK Y-00 cipher signals at λ_S = 1,550.1 nm with a phase level of 2^{16} (=65,536). In the QDSR process, truly random phase rotation was added in which the angle was determined by the TRNs generated from a spatially multiplexed 100 Gbit/s QRNG, based on vacuum fluctuation [12]. The 5 Gb/s PSK Y-00 cipher signals were polarization-multiplexed, using an emulator to generate 10 Gb/s DP PSK Y-00 cipher signals. The cipher signals, residing in an optical fiber, were transmitted to free space through FSO #1. A laser beam, of diameter 12 mm, was directed through a laser window hole on the left side of a fog chamber [13]. Further details of the FSO system can be obtained from [14]. A photo of the fog chamber without fog is shown in the inset of Fig. 3. The chamber width, corresponding to the transmission distance of the laser beam in the fog, was L_0 = 108 cm. Artificial fog with a particle size of approximately 3 mm, generated by an ultrasonic atomizer (Honda Electronics Co. Ltd., Ultrasonic atomizer unit JM-200), was injected into the chamber from a window hole at the top. The inflow amount of fog was maintained constant throughout the experiment. The laser beam was output from a laser window hole on the right side of the chamber and directed into an optical fiber through FSO #2. The power loss from the fiber input of FSO #1 to the fiber output of FSO #2 was measured to be 8.7 dB in the absence of fog. The additional loss was monitored every 5 s using an optical power meter at the output end of FSO #2. Transmission through an SMF of length 25 km was followed by FSO #2 to demonstrate transparent transmission over free space and fiber links. The measurements were conducted by gradually increasing the fog density from a fog-free state. Once the additional loss owing to the fog reached 20 dB, the inflow of fog was terminated. The measurements continued until the fog was eliminated.

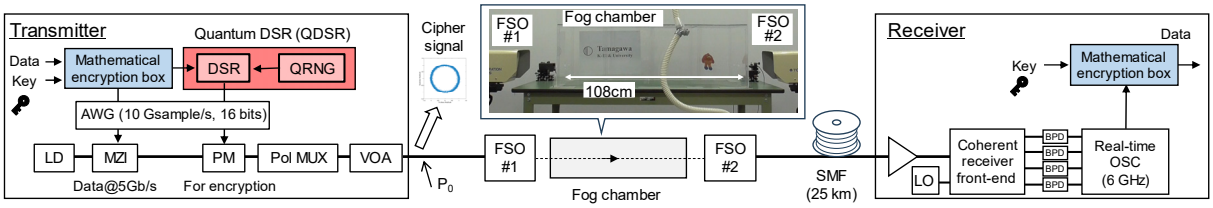

Fig. 3. Schematic of the experimental setup for Y-00 cipher transmission under dense fog conditions.

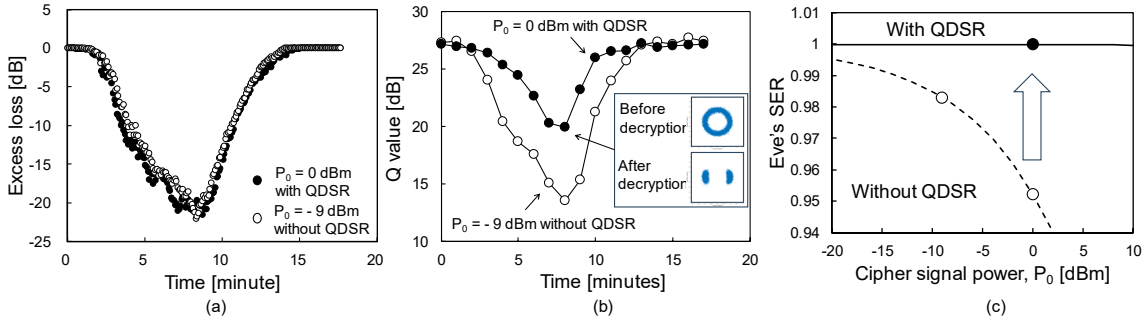

Fig. 4. (a) Additional loss by artificial fog in the fog chamber. (b) Q values for a 10 Gb/s DP PSK Y-00 cipher. (c) Eve's SERs

Figures 4(a) and (b) shows the experimental results for the input power P_0 of 0 dBm with QDSR and −9 dBm without QDSR. In Fig. 4(a), the filled and open circles depict the additional losses caused by the fog chamber for P_0 = 0 dBm with QDSR and P_0 = −9 dBm without QDSR, respectively. The additional losses reached 20 dB after approximately 8 min of fog generation. Then, after the fog generator was shut off, the fog cleared in approximately 7 min. In the receiver, the cipher signal was received by an intradyne coherent receiver and then subjected to offline digital signal processing to recover the original BPSK signals using the shared key. Data were stored each minute, and the Q values were calculated from the BPSK signals. Figure 4(b) shows the Q values and constellations before and after decryption with P_0 = 0 dBm with QDSR. The distribution of recovered BPSK signals is slightly larger in the vertical direction than in the horizontal direction due to the residual phase randomization effect of QDSR. The Q values for P_0 = −9 dBm without QDSR (open circles) and P_0 = 0 dBm with QDSR (filled circles) decrease as the fog density increases, reaching 13.5 and 20 dB, respectively, at the maximum additional loss, approximately 20 dB. Thus, the loss budget for free-space transmission increases with increasing optical power, even when QDSR causes an additional penalty while enhancing the security. This demonstrates that cipher communication is possible even in denser fog. The security of the system was assessed using the lowest SER reachable by Eve, assuming the worst conditions in which all signal power is tapped by Eve. The SER approaches 1 when signal discrimination completely fails, indicating a high level of security [8]. Eve's SERs for various optical input powers are shown in Fig. 4(c). The lowest Eve's SER without QDSR for P_0 = −9 dBm is estimated to be 0.983, while that for P_0 = 0 dBm is even worse at 0.952. In contrast, the lowest Eve's SER with QDSR is 0.999 for P_0 = 0 dBm. Thus, an increase in the loss budget and security enhancement was simultaneously achieved with QDSR. Furthermore, a high SER closely approaching 1 was maintained, even at a higher signal power as well as a lower power, as shown by the solid line. This indicates that QDSR provides high security throughout the entire link of FSO transmission.

4. Conclusions

We demonstrated security enhancement and higher loss budget in an FSO Y-00 cipher transmission system with QDSR under artificially generated dense fog conditions with a high attenuation of 20 dB. A 10 Gb/s DP PSK Y-00 cipher with QDSR was successfully transmitted over a 108 cm fog channel and in a 25 km SMF. A high level of security was achieved throughout the entire system, despite the increased signal power for a higher budget.

The authors would like to acknowledge G. Masada for his help in constructing the fog chamber. This work was partly supported by Innovative Science and Technology Initiative for Security Grant Number JPJ004596, ATLA, Japan, and the Air Force Office of Scientific Research under award number FA2386-22-1-4030.

References

[1] K. Matsuda, et al., *J. Lightwave Technol.*, **40**, 1494 (2022).
[2] F. P. Guiomar, et al., *J. Lightwave Technol.*, **40**, 3173 (2022).
[3] M. Z. Chowdhury, et al., *Open J. Commun. Soc.*, **1**, 957 (2020)
[4] G. Barbosa, et al., *Phys. Rev. Lett.* **90**, 227901 (2003).
[5] G. S. Kanter, et al., IEEE Comm. Mag., **47**, 74 (2009).
[6] O. Hirota, et al., *Phys. Rev. A*, 72, 022335 (2005).
[7] F. Futami, et al., ECOC 2023, We.C.7.4 (2023).
[8] K. Tanizawa, et al., *Opt. Express*, **29**, 10451(2021).
[9] F. Futami, et al., CLEO 2022, JW3B.107, (2022).
[10] G. S. Kanter, et al., Proc. SPIE 5842 (2005).
[11] K. Kato, Proc. SPIE 9980, 998005 (2016).
[12] K. Tanizawa, et al., *Photon. Technol. Lett.*, **35**, 229 (2023).
[13] G. Masada, Proc. SPIE 12238, 1223804 (2022),
[14] A. Bekkali, et al., *J. Lightwave Technol.*, **40**, 1509 (2022).