Secure Unrepeated Fiber Transmission with Quantum Deliberate Signal Randomization on Y-00 Protocol

Fumio Futami[1*], Ken Tanizawa[1], Kentaro Kato[1], Yuki Kawaguchi[2], and Shin Sato[2]
[1] *Quantum ICT Research Institute, Tamagawa University, 6-1-1 Tamagawa-gakuen, Machida, Tokyo, 194-8610, Japan*
[2] *Sumitomo Electric Industries, Ltd., Sakae-ku, Yokohama 244-8588, Japan*
**futami@lab.tamagawa.ac.jp*

Abstract: We demonstrate security-enhanced 10-Gbit/s PSK Y-00 cipher transmission with deliberate signal randomization driven by a quantum random number generator in a 362 km ultra-low-loss fiber link without optical amplifiers. High security is achieved at high optical powers. © 2022 The Author(s)

1. Introduction

Quantum technology has promising applications in secure optical fiber communications, providing extremely high security. Quantum key distribution (QKD) is a well-known application that securely shares a common key between authorized parties. Quantum technology is also applicable to data encryption. The quantum noise randomized stream cipher, called αη [1,2] or Y-00 [3], is symmetric-key encryption that prevents data interception using an eavesdropper (Eve). It utilizes extremely high-order modulation, and quantum mechanical non-orthogonality occurs even for a high-power coherent state signal if the modulation order is sufficiently high [4]. The non-orthogonality disables the correct discrimination of extremely high-order signals. Fig. 1 illustrates the concept of a secure optical fiber communication system with Y-00 cipher. Low-order data modulated signals, BPSK in the figure, are converted to high-order optical PSK signals based on a prescribed Y-00 protocol using a pre-shared key [5]. Following encryption, the modulation order is so high that quantum noise masks the adjacent signals, and Eve fails to perform signal discrimination. Meanwhile, the legitimate receiver with the pre-shared key converts the high-order PSK signals to the original BPSK signals. Since quantum noise is inherent and truly random in optical detection, signal masking using quantum noise is important for guaranteeing security. It imposes unavoidable uncertainty on Eve. The Y-00 cipher system features highly secure optical transmission without significantly sacrificing the data rate and reach. For instance, the system using digital coherent technology successfully completed single-channel 40-Gbit/s PSK Y-00 cipher transmission over 10,000 km [6] and 160-Gbit/s QAM Y-00 cipher transmission over 320 km [7]. The transmission capacity was increased by wavelength-division multiplexing (WDM) [8], and an aggregate capacity of 10 Tbit/s was demonstrated [9]. The security realized by signal masking is related to the optical power, bandwidth, and modulation order of the cipher. Lower optical power is suitable for higher security; however, it limits the signal quality or reach. Recently, the authors proposed a method to enhance the security of Y-00 cipher in the high optical power regime, named quantum deliberate signal randomization (QDSR). The proposed method additively randomizes signals using truly random numbers (TRNs) generated from a quantum random number generator (QRNG). The method was experimentally demonstrated in a configuration where the 5-Gb/s PSK Y-00 cipher transmitter and receiver were directly connected [10]. However, fiber transmission has not yet been demonstrated.

In this paper, we applied the Y-00 cipher system with QDSR to a fiber transmission system without inline optical amplifiers. Despite requiring high-power signals, such an unrepeated system is desirable as it provides a cost-effective solution for point-to-point connections over several hundred kilometers. Security-enhanced 10-Gbit/s dual polarization (DP) PSK Y-00 cipher transmission with QDSR is experimentally demonstrated over a 362 km ultra-low-loss pure silica core fiber. Owing to QDSR, sufficient signal masking or high security is achieved over the entire system even with a high signal input power of 5 dBm. The bit error rates (BERs) of the legitimate receiver are also investigated to establish that adequate signal quality is achievable.

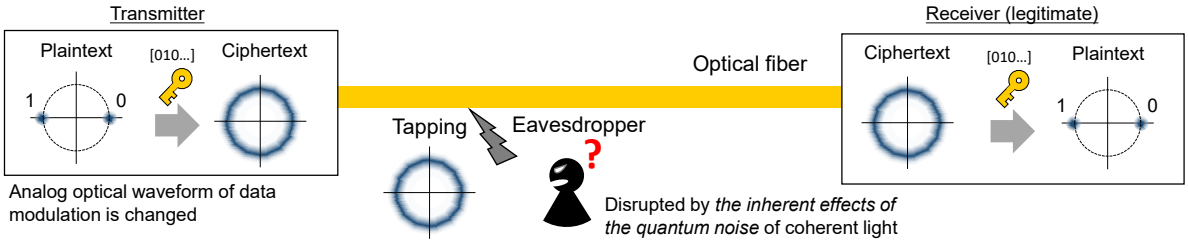

Fig. 1. Concept of Y-00 cipher in which a cipher signal is masked by quantum noise and is protected from eavesdropping.

2. Deliberate Signal Randomization Driven by a QRNG

A schematic overview of a Y-00 cipher system with QDSR is displayed in Fig. 2. The transmitter and receiver share a short key and a pseudorandom number generator (PRNG) in the mathematical encryption box. A QDSR is installed in the transmitter. Fig. 3 illustrates the operating principle of Y-00 cipher with QDSR for BPSK data modulation. Data are encrypted by rotating the phase of BPSK in a bit-by-bit manner. The PRNs extended from the pre-shared key determine the rotation angle ($-\pi/2 < \theta_{basis}(i) < \pi/2$). Following the encryption, the constellation becomes a high-order PSK signal with the phase of $\theta_{basis}(i)$, as shown in Fig. 3(ii). Subsequently, a truly random phase rotation of $\theta_{QDSR}(i)$, which is determined based on TRNs from a QRNG, is added to the signal, as shown in Fig. 3(iii). The range of QDSR phase rotation for 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. In total, the phase of each signal is rotated by $\theta_{basis}(i)+\theta_{QDSR}(i)$. In the receiver, a legitimate receiver holding the pre-shared key can detect the original BPSK signal by subtracting $\theta_{basis}(i)$ in a bit-by-bit manner, as depicted in Fig. 3(iv). Signal overlapping or uncertainty remains even for a legitimate receiver because TRNs for the QDSR phase shift are not shared between the transmitter and receiver.

Figs. 4 and 5 compare the masking effects with and without QDSR. Quantum noise, indicated with a dotted circle, masks the adjacent signals. The masking effect without QDSR is quantified using a masking number defined as $\Gamma_0 = \Delta\phi_{QN}/\Delta\theta_{basis}$, where $\Delta\phi_{QN}$ and $\Delta\theta_{basis}$ represent the phase uncertainty by quantum noise and the resolution of phase rotation angle, respectively. Γ_0 is proportional to 2^m and $1/\sqrt{P_0}$, where m and P_0 indicate the bit resolution of the phase rotation and signal power, respectively [6]. Although m is set at the largest possible value for maximal secrecy, P_0 is set to less than 0 dBm to maintain the signal security in a conventional system. As shown in Fig. 5, the QDSR phase shift causes signal overlapping. In addition to quantum noise, the phase uncertainty independent of P_0 is imposed on Eve's signal reception, strengthening the security. The masking number with QDSR is expressed as $\Gamma_{QDSR} = (\Delta\phi_{QN}+\pi\cdot\gamma_{QDSR})/\Delta\theta_{basis}$ [10]. By setting γ_{QDSR} to a few tens of percentages, Γ_{QDSR} can be made sufficiently large, and the security is high even at high optical powers. We note that the power can be increased as long as the quantum mechanical non-orthogonality remains, that is, the masking by quantum noise remains because QDSR does not increase the quantum noise; instead, it manipulates the phase of signals by using TRNs from a QRNG so that the phase is truly random for enhancing security.

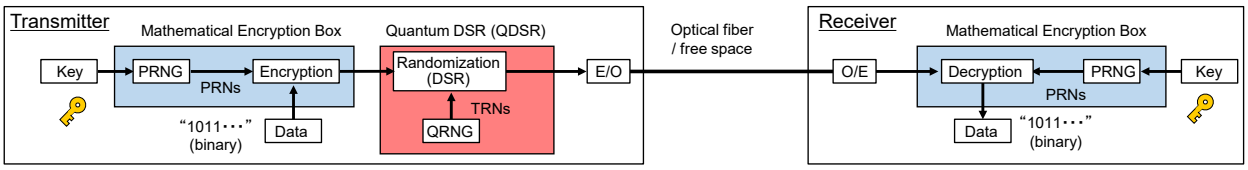

Fig. 2. Schematic of the Y-00 cipher system with QDSR.

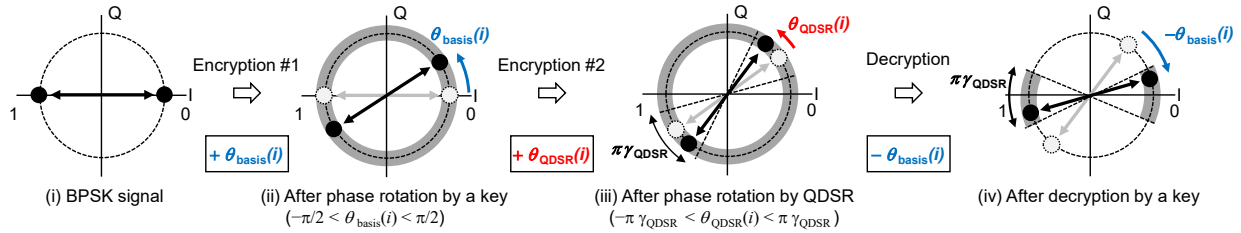

Fig. 3. Operating principle of the Y-00 cipher system with QDSR for BPSK data modulation. (i) BPSK signal. (ii) After phase rotation in the mathematical encryption box. (iii) After phase rotation by QDSR. (iv) After decryption in the receiver.

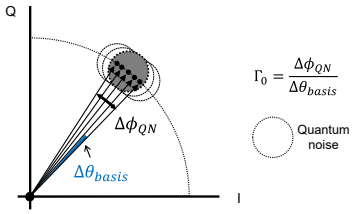

Fig. 4. Masking by quantum noise.

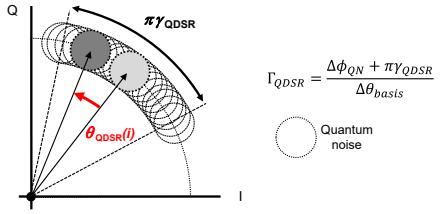

Fig.5. Masking by quantum noise and QDSR.

3. Transmission Experiment

We demonstrate an unrepeated 10-Gbit/s DP PSK Y-00 cipher system with QDSR in a 362 km fiber transmission link. Fig. 6 displays the experimental setup. Data and a pre-shared seed key of 256 bits were placed into a mathematical encryption box. The encryption box, which was implemented offline, included a PRNG for key-based

phase rotation. The rotation angles $\theta_{basis}(i)$ with m = 15 were generated according to the prescribed protocol [5]. In the QDSR, truly random phase rotation was added, where the angle was determined by the TRNs generated from a spatially multiplexed QRNG based on vacuum fluctuation for a high generation rate of 100 Gb/s [11]. The QDSR consumed up to 15-bit TRNs for each symbol, and a maximum throughput of 5 Gbit/s × 15 bits = 75 Gbit/s was required for each polarization to achieve real-time operation. The QRNG satisfied the requirement, although pre-stored TRNs were used for the offline processing. The outputs from the encryption box and QDSR were used for driving the optical modulators via an arbitrary waveform generator. The transmission fiber comprised six ultra-low-loss silica core fiber spools with a loss of 0.147 dB/km and A_{eff} of 130 μm^2. Each fiber length is 60.4 km and fiber spools with SMF pigtails were connected using an adapter. A conventional intradyne coherent receiver was utilized for signal detection, followed by offline digital signal processing including decryption [6].

Constellations before and after decryption with P_0 = 5 dBm and γ_{QDSR} = 0.2 are shown in the inset of Fig. 7(a). BPSK signals were recovered using the key information. Fig. 7(a) illustrates the BER characteristics of the legitimate receiver for γ_{QDSR} = 0, 0.2, and 0.4. All the measured BERs are below the typical SD-FEC threshold of 1.9×10^{-2}. The power penalties from a reference BPSK are less than 1 dB for γ_{QDSR} 0 and 0.2. Thus, encryption and decryption were achieved with minimal impact on the signal quality for a small γ_{QDSR}. Fig. 7(b) illustrates the BER of the legitimate receiver and masking numbers at P_0 = 5 dBm. For a larger γ_{QDSR}, a higher masking number or higher security was obtained while the BER increased because of the residual phase randomization of QDSR. This tradeoff should be carefully considered in the fiber transmission system. The BER and the masking number for γ_{QDSR} = 0.2 are 5.2×10^{-3} and ~6,000, respectively. Eve's symbol error rate (SER) for γ_{QDSR} = 0.2, calculated from the masking number, in different tapping points of the fiber link is depicted in Fig. 7(c). Without QDSR (dashed line), SER was at least 0.8933 at the transmitter end. It increased as the transmission distance increased because P_0 decreased owing to the loss in optical fibers. By contrast, SER with QDSR of γ_{QDSR} = 0.2 (solid line) exceeded 0.9998 in the full link. Thus, it can be concluded that QDSR provides high security with a small power penalty in the unrepeated fiber transmission requiring high optical power.

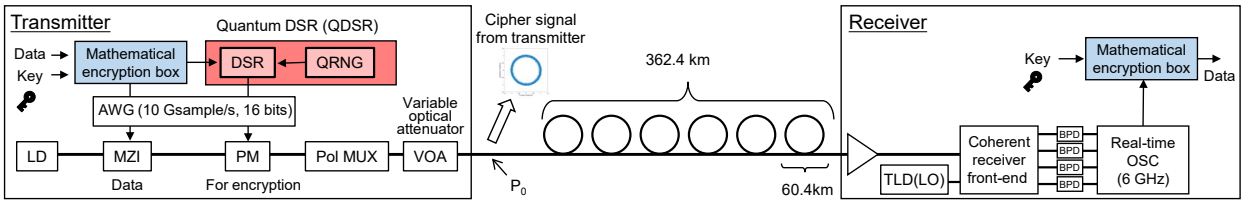

Fig. 6. Experimental setup of 10-Gb/s DP BPSK Y-00 cipher for a repeater-less transmission over 362 km.

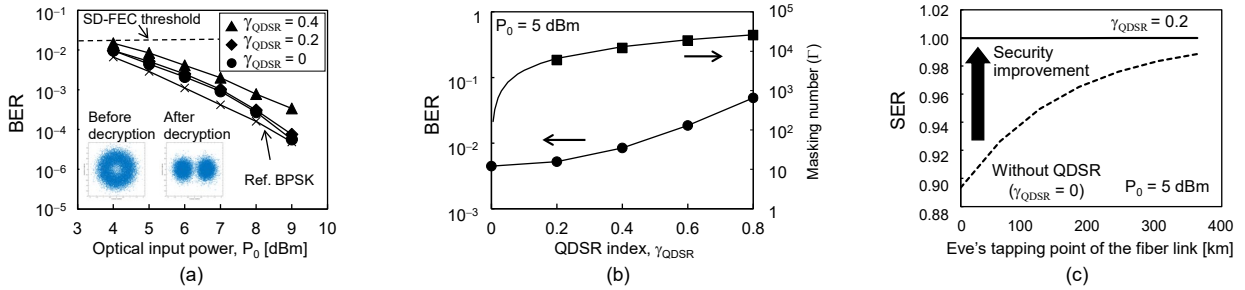

Fig. 7. (a) BER dependency on optical input powers. (b) BER and masking number for QDSR index. (c) Masking number at Eve's tapping point of the fiber link.

4. Summary

We demonstrated a 10-Gbit/s DP BPSK Y-00 cipher system with QDSR for enhancing the security of high optical power signals. The Y-00 cipher was applied to the unrepeated transmission of a 362 km ultra-low-loss silica core fiber that required high optical power (>5 dBm). Owing to QDSR, Eve's SER was maintained at nearly one in the full link. Low BERs of the legitimate receiver revealed that QDSR achieved high power and secure transmission.

This work was partly supported by Innovative Science and Technology Initiative for Security Grant Number JPJ004596, ATLA, Japan.

References

[1] G. Barbosa, et al., *Phys. Rev. Lett.* **90**, 227901 (2003).
[2] G. S. Kanter, et al., IEEE Comm. Mag., 47(11), 74(2009).
[3] O. Hirota, et al., *Phys. Rev. A*, 72, 022335 (2005).
[4] K. Kato, *Entropy* 24(5), 581(2022).
[5] F. Futami, et al., *J. Lightwave Technol.*, **38**, 2773(2020).
[6] K. Tanizawa, et al., *Opt. Express*, 29(7), 451(2021).
[7] X. Chen, et al., *Opt. Express* 29(4), 5658 (2021).
[8] F. Futami, *Quantum Inf. Process.* **13**, 2277 (2014).
[9] M. Yoshida, et al., *J. Lightwave Technol.*, **39**, 1056 (2021).
[10] F. Futami, et al., CLEO 2022, JW3B.107, (2022).
[11] K. Tanizawa, et al., CLEO 2022, AM3D.6, (2022).