ISSN 2186-6570

Transmission of Y-00 Quantum Noise Stream Cipher with Quantum Deliberate Signal Randomization over Field-Installed Fiber

Fumio Futami, Ken Tanizawa and Kentaro Kato

Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610 Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.13, No.1, 23-25, 2023

Transmission of Y-00 Quantum Noise Stream Cipher with Quantum Deliberate Signal Randomization over Field-Installed Fiber

Fumio Futami, Ken Tanizawa and Kentaro Kato
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa Gakuen, Machida, Tokyo, 194-8610, Japan
E-mail: futami@lab.tamagawa.ac.jp

***Abstract*— This study presents the optical fiber transmission of the Y-00 quantum stream cipher with quantum deliberate signal randomization (QDSR). QDSR driven by a quantum random number generator significantly improves signal masking utilizing quantum noise to enhance security. We transmitted a 10-Gb/s line-rate dual-polarization phase-shift keying Y-00 cipher with QDSR over a 400-km field-installed single-mode fiber link. When the number of encryption phase levels is set to 2^{16}, the quantum noise masking number is much higher than that without QDSR, thereby enhancing security. As the QDSR index increases, the eavesdropper's probability of correctly detecting the signal decreases. After transmission, the measured bit error rates are below the typical soft-decision forward error correction threshold.**

***Index Terms*—Y-00 quantum stream cipher, deliberate signal randomization, physical cipher, secure optical communication.**

I. Introduction

The requirement for secure data communication is continuously becoming stricter and demanding. The utilization of encryption is a promising solution for data protection. The quantum noise stream cipher, called αη [1,2] or Y-00 [3], provides a symmetric-key direct data encryption system for secure fiber-optic communications.

The Y-00 cipher employs a multi-level optical modulation scheme to randomize cipher signals by quantum noise and prevents signal interception by an eavesdropper. The quantum noise masking number, defined as the number of cipher signal levels covered by quantum noise, is a security measure. A higher number leads to higher security. The additive noise, such as amplified spontaneous emission noise, also enhances the randomization of cipher signals. The number is proportional to the modulation order and inversely proportional to the square root of the cipher signal power. The maximum modulation order for 5 Gbaud or higher is 16 bits at most, which is limited by the number of digital-to-analog (DAC) bits. The Y-00 cipher with such a modulation order may not achieve a sufficiently high quantum noise masking number, depending on the signal power. To address this limitation, deliberate signal randomization (DSR) emerges as a technique to instill randomness into cipher signals and substantially augment noise masking [4]. Driving the DSR with pseudo-random numbers (PRN) allows pseudo-randomness to be added to cipher signals [5,6]. We showed analytically that DSR reduced the eavesdropper's correct signal detection probability [7]. In addition, we proposed and experimentally demonstrated a quantum DSR (QDSR), which is driven by a true random number (TRN) from a quantum random number generator to add true randomness to cipher signals for enhancing security [8]. We also demonstrated fiber transmission experiments involving the Y-00 cipher coupled with QDSR. A 10-Gb/s line-rate dual-polarization binary phase-shift keying (BPSK) Y-00 cipher with QDSR, featuring 2^{16} phase levels, was deployed for transmission over field-installed standard single-mode fibers (SMFs) spanning a 400-km distance and utilizing optical amplifiers. When the QDSR index was set to 0.2, the quantum noise masking number exceeded that without QDSR by more than 40 times, thus enhancing security with minimal compromise to signal transmission quality [9].

Here, we further investigate security and transmission quality for higher QDSR indexes in a 400-km-long optical fiber installed on our campus. The quantum noise masking increases with higher QDSR indexes, indicating that higher security is provided, and still, the bit error ratios of dual-polarization BPSK Y-00 cipher signals with QDSR after the transmission are below the typical soft-decision forward error correction threshold.

II. Quantum Deliberate Signal Randomization

A schematic overview of a Y-00 cipher system with QDSR is presented in Fig. 1. The transmitter and receiver share a short key and a PRN generator (PRNG) for both encryption and decryption processes. The transmitter incorporates QDSR. Figure 2 illustrates the operational concept of a Y-00 cipher with BPSK data modulation. Data encryption involves rotating the phase of phase-shift keying (PSK) in a bitwise manner. The rotation angle ($-\pi/2 < \theta_{\mathrm{basis}(i)} < \pi/2$) is randomly determined by PRNs derived from the pre-shared key. Here, *i* denotes the identification of a BPSK signal. Post-encryption phase rotation transforms the constellation into a high-order PSK signal, as depicted in Fig. 2 (ii). The PSK signal order is 2^{m+1}, with a rotation angle resolution of $\Delta\theta_{\mathrm{basis}} = \pi/2^{m}$ or *m* bits. The value of *m* is set to the maximum achievable level for optimal secrecy. Intuitively, noise hampers eavesdropping attempts aimed at accurately detecting high-order PSK signals (e.g., 32,768 PSK for m = 15). In contrast, a legitimate receiver with the pre-shared key can recover the original BPSK signal by subtracting $\theta_{basis(i)}$ bitwise. m is chosen as a sufficiently large number to ensure that adjacent signals are masked by quantum noise.

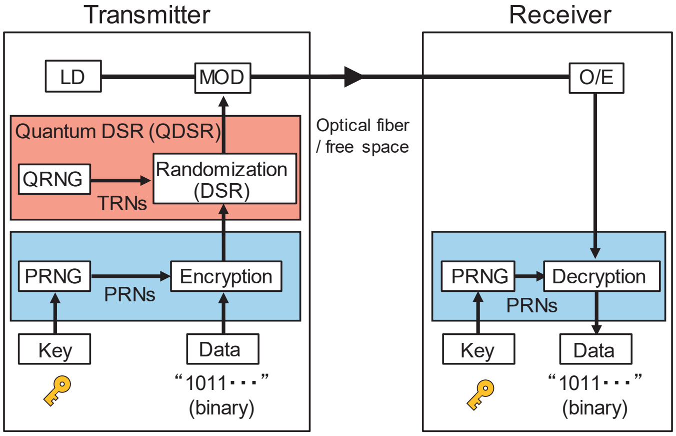
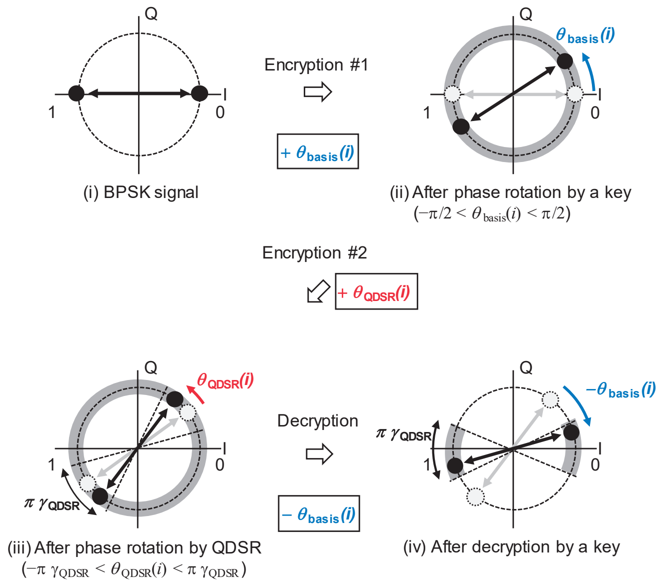


Fig. 1. Schematic of Y-00 cipher system with DSR driven by quantum random generator



(i) BPSK signal

(ii) After phase rotation by a key ($-\pi/2 < \theta_{\text{basis}}(i) < \pi/2$)

(iii) After phase rotation by QDSR ($-\pi\ \gamma_{\text{QDSR}} < \theta_{\text{QDSR}}(i) < \pi\ \gamma_{\text{QDSR}}$)

(iv) After decryption by a key

Fig. 2. Operating principle of Y-00 cipher system with QDSR for BPSK data modulation: (i) BPSK signal, (ii) after phase rotation in mathematical encryption box, (iii) after phase rotation by QDSR, and (iv) after decryption in receiver.

The security offered by quantum noise-based signal masking is immutable and inescapable, given that quantum noise is genuinely random and inherent during detection. The level of masking for secrecy is quantified by defining a quantum masking number (Γ_0) as

$$\Gamma_0 = \frac{\Delta\varphi_{shot}}{\Delta\theta_{basis}} \tag{1}$$

where

$$\Delta\varphi_{shot} = \sqrt{\frac{2h\upsilon_0 R}{\eta_q P_0}} \tag{2}$$

with h, υ_0, R, η_q, and P_0 representing the Planck constant, signal frequency, electrical signal bandwidth, quantum efficiency of the photodetector, and optical power of the signal, respectively [10]. Without DSR, Γ_0 is directly proportional to 2^m. Consequently, the security level can be constrained by the bit resolution of the DAC.

QDSR is a keyless randomization technique that augments quantum noise masking. In QDSR, a random phase rotation ($\theta_{QDSR(i)}$), determined by TRNs generated from a QRNG, is added to each signal, as depicted in Fig. 2 (iii). The range of the QDSR phase rotation for a BPSK-based Y-00 cipher is $\pi\cdot\gamma_{QDSR}$, where γ_{QDSR} represents the depth of randomization. Because QDSR relies on TRNs, genuinely random phase uncertainty is introduced into quantum noise masking. Hence, the phase of each data signal is rotated by $\theta_{basis(i)} + \theta_{QDSR(i)}$, leading to signal overlap in the constellation after encryption, as illustrated in Fig. 2 (iii). Figure 2 (iv) demonstrates that this signal overlap or uncertainty persists even after a legitimate receiver subtracts $\theta_{basis(i)}$ during decryption. This is because the TRNs for the QDSR phase shift are not shared between the transmitter and receiver. Consequently, truly random phase uncertainty makes illegitimate signal reception difficult, thereby enhancing security. However, it does reduce signal quality for the legitimate receiver.

We define the masking number (Γ_{QDSR}) of BPSK Y-00 cipher signals with QDSR as

$$\begin{aligned}\Gamma_{QDSR} &= \frac{\Delta\varphi_{shot} + \pi\gamma_{QDSR}}{\Delta\theta_{basis}}. \\ &= \Gamma_0 + \frac{\pi\gamma_{QDSR}}{\Delta\theta_{basis}}\end{aligned} \tag{3}$$

The second term is independent of the signal power. Therefore, when $\Delta\varphi_{shot} \ll \pi\gamma_{QDSR}$, Γ_{QDSR} is independent of the signal power.

The quantum noise masking number, Γ_0, was 148 for R = 5 Gbit/s and m = 15 without QDSR when $P_0 = -19$ dBm. In contrast, the quantum noise masking numbers with QDSR, Γ_{QDSR} were 6.8×10^3, 1.3×10^4, and 2.0×10^5 for QDSR indexes of $\gamma_{QDSR} = 0.2$, 0.4 and 0.6, respectively. They are significantly higher than those without QDSR. Compared with the quantum noise masking number without QDSR, they are more than 45, 90, and 135 times greater, respectively. This result underscores the enhancement of security via QDSR, even though it poses limits on DAC bit resolution. A minimum DAC resolution is required to achieve signal masking utilizing quantum noise because QDSR can only amplify the effect of quantum noise signal masking.

III. EXPERIENT

For evaluating the transmission performance of BPSK Y-00 cipher signals with QDSR, we conducted a transmission experiment of a 10-Gb/s line-rate dual-polarization Y-00 cipher system with QDSR based on BPSK data modulation in a 400-km fiber transmission link. The experimental setup is depicted in Fig. 3. The data and a pre-shared seed key were input into a mathematical encryption module. This offline encryption module incorporated a pseudo-random number generator (PRNG) for random phase rotation based on the key. The rotation angles $\theta_{\mathrm{basis}(i)}$ with a value of m = 15 was generated following a prescribed protocol [11].

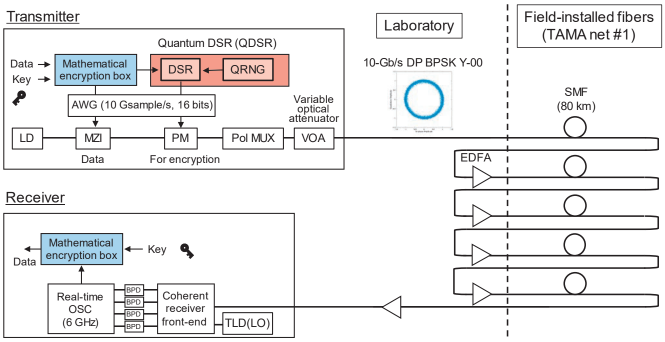


Fig. 3. Experimental setup of 10-GB/s dual-polarization BPSK Y-00 cipher transmission utilizing quantum DSR in field-installed optical fiber link for 400 km.

In the QDSR process, true random phase rotation was introduced, where the angles were determined by TRNs generated from a spatially multiplexed QRNG based on vacuum fluctuation, achieving a high generation rate of 100 Gb/s [12]. The QDSR necessitated 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 enable real-time operation. The QRNG met this requirement; however, it relied on pre-stored TRNs. The outputs from the encryption module and QDSR were utilized to drive the optical modulators through an arbitrary waveform generator. A variable optical attenuator was employed to adjust the optical power emitted from the transmitter.

The transmission fiber link comprised five sets of field-installed standard SMFs, each spanning 80-km long, and included erbium-doped fiber amplifiers. The input power into the SMF was set at $P_0 = -19$ dBm. In the receiver, the cipher signals were detected utilizing a conventional intradyne coherent receiver, followed by offline digital signal processing for decryption and carrier phase recovery (CPR) [8]. A straightforward CPR method, based on calculating the power of the received phase, was effective for decrypting BPSK signals with residual random phase shifts, provided that the average number of processed symbols was set to approximately 100. The evaluation encompassed processing more than 1.1 million BPSK signals. The quantum noise masking numbers Γ_{QDSR} for γ_{QDSR} = 0.2, 0.4, and 0.6 exceeded 6.9×10^3, 1.3×10^4, and 2.0×10^4, respectively. They were over 63, 125, and 187 times higher than that without QDSR, respectively. The substantial quantum noise masking numbers cannot be achieved solely through quantum noise masking. The probability of an eavesdropper correctly detecting a cipher signal is approximately $\Gamma^{-1} = 1.5 \times 10^{-4}$, $7.6 \times 10^{-5,}$ and 5.1×10^{-5} for γ_{QDSR} = 0.2, 0.4, and 0.6, indicating an exceedingly low likelihood of successful eavesdropping. Subsequently, we investigated the impact of residual masking on signal quality. After transmission, the original BPSK signals were recovered from the Y-00 cipher signals. To quantitatively assess signal quality, the bit error rates (BERs) were calculated. BERs with γ_{QDSR} = 0.2, 0.4, and 0.6 were 8.1×10^{-5}, 3.2×10^{-4}, and 2.5×10^{-3}, respectively. As γ_{QDSR} increased, BER increased owing to the crosstalk due to QDSR. Still, they are well below the typical soft-decision forward error correction threshold (SD FEC) of 1.9×10^{-2}.

IV. Summary

We demonstrated optical fiber transmission for the Y-00 quantum stream cipher with QDSR. QDSR significantly improved signal masking through quantum noise, thereby achieving heightened security. We successfully transmitted a 10-Gb/s line-rate dual-polarization PSK Y-00 cipher with QDSR through a 400-km SMF link on campus. Higher security was achieved as the QDSR index increased to 0.2, 0.4, and 0.6. BERs after transmission were smaller than the SD FEC threshold. This outcome demonstrates that the Y-00 cipher transmission system with QDSR enhances security while maintaining sufficient transmission performance.

V. Acknowledgement

Part of this work was supported by the Innovative Science and Technology Initiative for Security, Grant Number JPJ004596, ATLA, Japan.

References

[1] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure Communication Using Mesoscopic Coherent States," Phys. Rev. Lett., vol.90, 227901, June 2003.

[2] G. S. Kanter, D. Reilly and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," IEEE Comm. Mag., vol. 47, no. 11, pp. 74-81, November 2009.

[3] 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, vol.72, 022335, August 2005.

[4] H. P. Yuen, "KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation," https://arXiv:quant-ph/0311061v6, 2003.

[5] G. S. Kanter, E. Corndorf, C. Liang, V. S. Grigoryan, and P. Kumar, "Exploiting quantum and classical noise for securing high-speed optical communication networks," Proc. SPIE 5842, Fluctuations and Noise in Photonics and Quantum Optics III, May 2005.

[6] K. Kato, "Quantum enigma cipher as a generalization of the quantum stream cipher," Proc. SPIE 9980, Quantum Communications and Quantum Imaging XIV, 998005, September 2016.

[7] F. Futami, K. Tanizawa and K. Kato, "Analysis of Eavesdropper's Correct Signal Detection Probability for BPSK Y-00 Quantum Stream Cipher with Deliberate Signal Randomization," Tamagawa University Quantum ICT Research Institute Bulletin, vol.12 no.1, pp.11-14, 2022.

[8] F. Futami, K. Tanizawa, and K. Kato, "Experimental Demonstration of Quantum Deliberate Signal Randomization for Y-00 Quantum Noise Stream Cipher," in Conference on Lasers and Electro-Optics (CLEO), paper JW3B.107, 2022.

[9] F. Futami, K. Tanizawa, and K. Kato, "Field-installed fiber transmission of Y-00 quantum noise stream cipher with quantum deliberate signal randomization," Proc. SPIE 12429, Next-Generation Optical Communication: Components, Sub-Systems, and Systems XII, 124291J, March 2023.

[10] K. Tanizawa and F. Futami, "Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system," Opt. Express, vol.29, pp.10451-10464, 2021.

[11] 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," IEEE/OSA Journal of Lightwave Technology, vol. 38, no. 10, pp. 2773-2780, May 2020.

[12] K. Tanizawa, K. Kato, and F. Futami, "Four-Channel Parallel Broadband Quantum Entropy Source for True Random Number Generation at 100 Gbps," in Conference on Lasers and Electro-Optics (CLEO), paper AM3D.6, 2022.