ISSN 2186-6570

Mitigating Tradeoffs between Signal Security and Transmission Reach in PSK Y-00 Quantum Stream Cipher with Deliberate Signal Randomization

Ken Tanizawa and Fumio Futami

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, 19-22, 2023

©Tamagawa University Quantum ICT Research Institute 2023
All rights reserved. No part of this publication may be reproduced in any form or by any means electronically, mechanically, by photocopying or otherwise, without prior permission of the copy right owner.

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.13 No.1 : 19–22 (2023)

Mitigating Tradeoffs between Signal Security and Transmission Reach in PSK Y-00 Quantum Stream Cipher with Deliberate Signal Randomization

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

***Abstract*—This study reports tradeoffs between the amount of uncertainty imposed on illegitimate signal reception and the maximum fiber transmission distance in a phase-shift keying (PSK) Y-00 quantum stream cipher system with deliberate signal randomization. We derive an analytical formula that shows the tradeoffs when a fiber link configuration and required optical signal-to-noise ratio at the receiver side are given. Numerical simulations using the formula in a long-haul terrestrial transmission system with a reach of ~3,000 km is shown.**

***Index Terms*— Y-00 quantum stream cipher, deliberate signal randomization, optical coherent transmission systems.**

I. Introduction

Signal interception from a fiber link is a security threat in optical fiber networks [1]. In a current optical communication system, coherent transceivers are equipped with symmetric key data encryption, such as the advanced encryption standard (AES) [2]. The security of AES is based on computational complexity: cryptanalysis of the encrypted digital data is hard to be successful, while illegitimate signal reception is not prevented. Physical layer encryption (PLE) is a signal-level symmetric-key encryption to directly protect signals from being intercepted and enhance the security of communication systems. The PLE utilizes unique signal encoding and/or modulation. Here, we focus on the encryption using the effect of quantum noise on optical signals [3], called alpha-eta [4] or Y-00 quantum stream ciphers [5].

The Y-00 cipher utilizes the synergistic effect of combining a symmetric-key-based high-order optical modulation and truly random quantum noise inevitable in the signal detection. Provided that the order of modulation is sufficiently high, for example, 2^{18} phase-shift keying (PSK) [6], quantum noise imposes true uncertainty on the encrypted high-order optical signals, and signal reception without a symmetric key or interception inevitably contains errors. The uncertainty is unavoidable, which is promised by the quantum mechanics. Thus, the signal security of Y-00 cipher is irreducible. This feature makes it different from the conventional symmetric-key encryption carrying potential risk of being compromised in the future. State-of-the-art experiments of Y-00 cipher in optical fiber communications demonstrated single-channel bit rate of higher than 100 Gbit/s [7],[8], long reach of 10,118 km at 40 Gbit/s in a single channel [9], and wavelength-division multiplexed high capacity of 10 Tbit/s [10]. Furthermore, the tradeoff between reach and signal security in PSK-based Y-00 cipher transmission over a linear and nonlinear fiber channel were theoretically investigated in [9] and [11], respectively.

Recently we have proposed quantum deliberate signal randomization (DSR) in which the encrypted high-order signal is additionally randomized based on the uncertainty generated using a quantum random number generator [12]. We have experimentally demonstrated PSK Y-00 cipher with the quantum DSR in a fiber transmission system with optical amplifiers [13] and an unrepeated fiber transmission system [14]. The DSR significantly enhances the security of the Y-00 cipher, while it affects signal quality or transmission reach because the additional uncertainty is not removable even for a legitimate receiver.

In this paper, we report tradeoffs between signal security and reach in a PSK Y-00 quantum stream cipher transmission system with DSR over a fiber link using optical amplifiers. A simple linear fiber channel model is employed, and an analytical tradeoff formula is derived. The formula shows the relation between the masking number which indicates the degree of signal security and reach when a fiber link configuration and required optical signal-to-noise ratio (OSNR) at the receiver side are given. We experimentally investigate the required OSNR for 10-Gbit/s dual-polarization PSK Y-00 cipher with DSR and numerically analyze the tradeoff in a terrestrial fiber link with a distance of ~3,000 km.

II. Theoretical Analysis

A. Signal masking in PSK Y-00 cipher with DSR

Y-00 cipher employs high-order modulation using a symmetric key. Fig. 1 shows the operating principles of PSK Y-00 cipher based on binary PSK message modulation ($M = 2$). Total 2^m bases are prepared for the encryption. One of them is selected based on the key information for one-bit modulation: phase of coherent light is modulated to 0 or π, $\theta_{\mathrm{data}}(i)$, on a bit-by-bit basis phase $\theta_{\mathrm{basis}}(i)$ between 0 and π. The encrypted signal follows a $M{\cdot}2^m$ PSK template, and constellation diagram becomes an extremely high-order PSK for a large m, as shown in Fig. 1(a). Fig. 1(b) indicates the magnified image of the encrypted signal. The adjacent bases are masked by quantum noise. Thus, an eavesdropper cannot correctly discriminate the encrypted signal carrying the message and key. A quantum

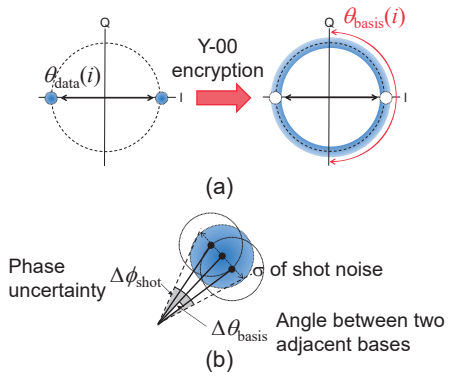

Fig. 1. Operating principles of PSK Y-00 cipher: (a) constellation diagrams and (b) magnified image.

noise masking number that indicates the number of signals masked by quantum noise is introduced as a security measure.

The quantum noise masking number for PSK Y-00 cipher $\Gamma_{\text{Q-psk}}$ is defined as the ratio of angle uncertainty imposed by quantum noise $\Delta\phi_{\text{shot}}$ to angle difference between adjacent bases $\Delta\theta_{\text{basis}}$ and expressed as

$$\Gamma_{\text{Q-psk}} = \frac{\Delta\phi_{\text{shot}}}{\Delta\theta_{\text{basis}}}. \tag{1}$$

The angle difference $\Delta\theta_{\text{basis}}$ for a data modulation order M and a bit number of bases m for the encryption is obtained as

$$\Delta\theta_{\text{basis}} = \frac{2\pi}{M \cdot 2^m}. \tag{2}$$

The angle uncertainty is given by

$$\Delta\phi_{\text{shot}} = \sqrt{\frac{2eB}{SP_S}}, \tag{3}$$

where e, B, S, and P_S are the elementary charge, receiver bandwidth, responsivity of a photodetector, and signal power, respectively [9]. The photodiode responsivity S is expressed as

$$S = \frac{\eta_q e}{h\nu_0}, \tag{4}$$

where η_q, h, and ν_0 are the quantum efficiency of a photodetector, Planck's constant, and optical carrier frequency, respectively.

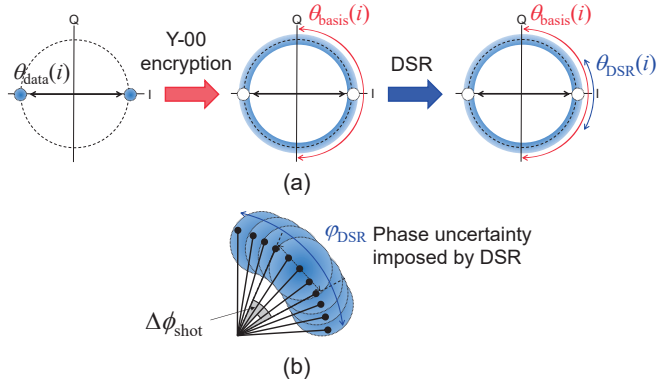

Fig. 2. Operating principles of PSK Y-00 cipher with DSR: (a) constellation diagrams and (b) magnified image.

DSR is a technique that enhances the security of Y-00 cipher. Fig. 2 shows the operating principles. Following the Y-00 encryption with a symmetric key, phase of the signal is randomized in a bit-by-bit manner based on unpredictable randomness generated using a physical random number generator. In other words, the phase is rotated by $\theta_{\text{DSR}}(i)$, where the angle is randomly determined using unpredictable random numbers. The constellation diagram after the encryption with DSR is similar, as shown in Fig. 2(a). Meanwhile, as shown in Fig. 2(b), the phase uncertainty by DSR φ_{DSR} is additionally imposed on the discrimination of the encrypted signals. The masking number for PSK Y-00 cipher with DSR is defined as

$$\Gamma_{\text{DSR\_psk}} = \frac{\Delta\phi_{\text{shot}} + \varphi_{\text{DSR}}}{\Delta\theta_{\text{basis}}}. \tag{5}$$

The phase uncertainty φ_{DSR} is the maximum range of phase rotation by the DSR and is expressed as

$$\varphi_{\text{DSR}} = \frac{2\pi}{M}\gamma_{\text{DSR}}. \tag{6}$$

Here, γ_{DSR} is the DSR index between 0 and 1, indicating the amount of signal randomization. By substituting Eqs. (2)-(4) and (6) into Eq. (5), the masking number is expressed as

$$\Gamma_{\text{DSR\_psk}} = \frac{M \cdot 2^m}{2\pi}\left(\sqrt{\frac{2h\nu_0 B}{\eta_q P_S}} + \frac{2\pi}{M}\gamma_{\text{DSR}}\right). \tag{7}$$

The effect of DSR on the masking number is independent of the signal power P_S. Thus, a high masking number can be achieved even at a high optical power regime. On the other hand, the effect cannot be eliminated for a legitimate receiver with the key, and hence transmission performances are degraded depending on the DSR index. It is important to appropriately set the value of γ_{DSR} considering the requirement of signal quality at the receiver side.

B. Tradeoffs between the masking number and reach

Here, we consider a long-haul optical fiber transmission system with optical fiber amplifiers. Fig. 3 shows the system configuration and power diagram. The fiber link consists of L km fiber spans and optical fiber amplifiers, and loss and gain are repeated in a regular manner. The number of spans is N, and the span loss is equal to the gain of the amplifier G. Provided

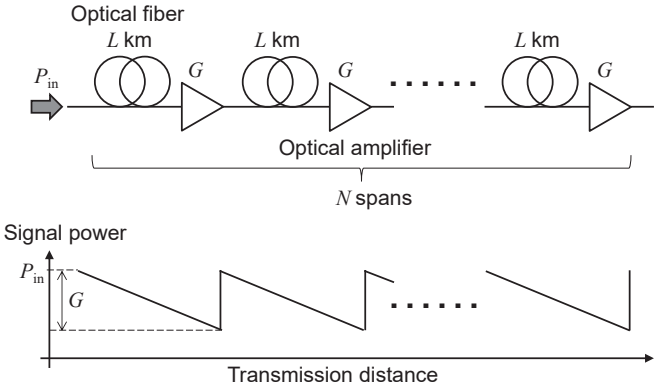

Fig. 3. Configuration of a fiber link with optical fiber amplifiers.

that the signal power launched into each fiber span and OSNR required for adequate signal quality at the receiver are P_{in} and $OSNR_{\text{req}}$, respectively, the achievable maximum number of spans N_{max} is given as

$$N_{\text{max}} = \left\lfloor \frac{P_{\text{in}}}{OSNR_{\text{req}} \cdot 2n_{\text{sp}} h\nu_0 \Delta\nu_{\text{noise}} G} \right\rfloor, \quad (8)$$

where n_{sp} and $\Delta\nu_{\text{noise}}$ are the spontaneous emission factor of the amplifier and noise bandwidth of OSNR, respectively [9]. The number of fiber spans is an integer, and floor function is used. Meanwhile, optical signal power P_{S} is obtained from Eq. (7) as

$$P_S = \frac{M^2 \cdot 2^m \cdot h\nu_0 B}{2\pi^2 \eta_{\text{q}} \left(\Gamma_{\text{DSR\_psk}} - \gamma_{\text{DSR}} \cdot 2^m\right)^2}. \quad (9)$$

We assume here that an eavesdropper detects all signal power at the input of the fiber link and hence define the masking number using P_{in}. By substituting (9) into (8) with a relation $P_{\text{in}} = 2P_{\text{S}}$ assuming a polarization multiplexing technique, the tradeoffs among the masking number, DSR index, and the maximum number of spans in the transmission system is derived as

$$N_{\text{Y-00\_DSR\_max}} = \left\lfloor \frac{M^2 \cdot 2^{2m} \cdot B}{2\pi^2 \cdot OSNR_{\text{req}} \cdot n_{\text{sp}} \eta_{\text{q}} \Delta\nu_{\text{noise}} G} \cdot \frac{1}{\zeta^2} \right\rfloor, \quad (10)$$

where

$$\zeta = \Gamma_{\text{DSR\_psk}} - \gamma_{\text{DSR}} \cdot 2^m. \quad (11)$$

It is worth noting that the required OSNR at the receiver $OSNR_{\text{req}}$ is related to the DSR index γ_{DSR} in the Y-00 cipher system with DSR.

III. Numerical Simulation

The required OSNR at a receiver side was experimentally defined in this study. Here the bit error ratio (BER) threshold for forward error correction was set to 1×10^{-3}. Fig. 4 shows the OSNR required to achieve the BER threshold for various DSR indexes in a 10-Gbit/s dual-polarization PSK Y-00 cipher system with DSR. The OSNR was defined in a noise bandwidth $\Delta\nu_{\text{noise}}$ of 0.1 nm. The message modulation before the encryption was binary PSK (M = 2). The bit number of bases for the encryption m was 15 bits. The requires OSNR $OSNR_{\text{req}}$ for each DSR index γ_{QDSR} was determined from this result.

Next, we used Eqs. (10) and (11) and numerically investigated the tradeoffs in a long-haul terrestrial optical communication system with a total transmission distance of ~3,000 km. Table 1 summarizes the system parameters. A fiber link consisted of 100-km span standard single mode fiber with a fiber loss of 0.18 dB/km and optical amplifiers with a noise figure of 5.0 dB. The amplifier gain G was 18 dB to compensate the link loss. Fig. 5 shows the relation between the masking number and transmission reach for various DSR indexes. The masking number at DSR index = 0 (without DSR) decreases for the increase in the transmission reach, because signal power launched into each fiber span increases to achieve the required OSNR at the receiver side. On the other hand, the DSR substantially increases the masking number, and the masking number is independent of the reach in practice. Thus, the DSR significantly enhances the signal security in the optical fiber transmission system using amplifiers.

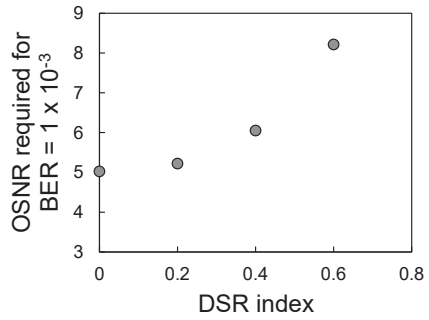

Fig. 4. OSNR required to achieve a BER of 1×10^{-3} for various DSR indexes in 10-Gbit/s dual-polarization PSK Y-00 cipher system with DSR.

TABLE I
Simulation Parameters of Long-Haul Fiber Transmission System

Item	Value
Fiber span length: L	100 km
Fiber loss	0.18 dB/km
Amplifier gain: G	18 dB
Noise figure of amplifier: $2n_{\text{sp}}$	5.0 dB
Quantum efficiency of a PD for eavesdropping: η_{q}	1

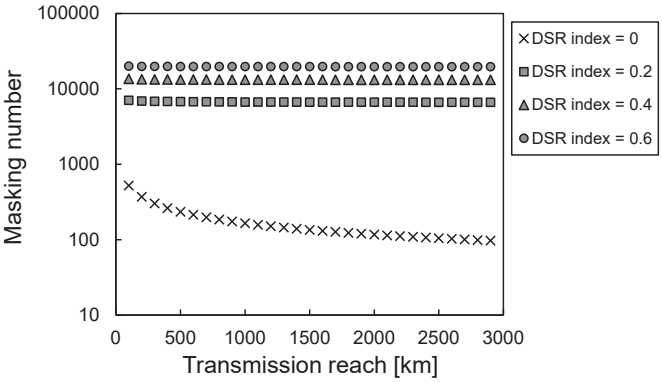

Fig. 5. Numerical analysis of the tradeoffs between the masking number and transmission reach for various DSR indexes in 10-Gbit/s dual-polarization PSK Y-00 cipher system with DSR.

IV. Conclusion

We have analyzed tradeoffs between the masking number and transmission reach in PSK Y-00 cipher with DSR. Provided that a fiber link consisted of regularly repeated loss and gain, due to fiber attenuation and optical amplification, an analytic formula of the tradeoffs was derived. Using the formula and experimental investigation of OSNR required at the receiver side, we numerically studied the relation between the masking number and reach in a 10-Gbit/s terrestrial long-haul (~ 3,000 km) fiber transmission system employing PSK Y-00 cipher with DSR. The results showed that the DSR significantly increased the masking number and mitigated the tradeoffs between the signal security and transmission reach.

Acknowledgment

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

REFERENCES

[1] N. Skorin-Kapov, M. Furdek, S. Zsigmond and L. Wosinska, "Physical-layer security in evolving optical networks," in IEEE Communications Magazine, vol. 54, no. 8, pp. 110-117, 2016. DOI: 10.1109/MCOM.2016.7537185.

[2] https://ii-vi.com/product/400g-cfp2-dco-digital-coherent-optics-transceiver/

[3] G. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," Phys. Rev. Lett., vol. 90, 227901, 2003. DOI: 10.1103/PhysRevLett.90.227901

[4] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen "Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks," Phys. Rev. A, vol. 71, 062326, 2005. DOI: 10.1103/PhysRevA.71.062326

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

[6] K. Tanizawa and F. Futami, "Single-channel 48-Gbit/s DP PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF," Opt. Express, vol. 27, pp. 25357-25363, 2019. DOI: 10.1364/OE.27.025357

[7] X. Chen, K. Tanizawa, P. Winzer, P. Dong, J. Cho, F. Futami, K. Kato, A. Melikyan, and K. W. Kim, "Experimental demonstration of a 4,294,967,296-QAM-based Y-00 quantum stream cipher template carrying 160-Gb/s 16-QAM signals," Opt. Express, vol. 29, pp. 5658-5664, 2021. DOI: 10.1364/OE.405390

[8] J. Sun, L. Jiang, A. Yi, J. Feng, X. Deng, W. Pan, B. Luo, and L. Yan, "Experimental demonstration of 201.6-Gbit/s coherent probabilistic shaping QAM transmission with quantum noise stream cipher over a 1200-km standard single mode fiber," Opt. Express, vol. 31, pp. 11344–11353 2023. DOI: 101364/OE.484431

[9] 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. DOI: 10.1364/OE.418302

[10] M. Yoshida, T. Kan, K. Kasai, T. Hirooka, and M. Nakazawa, "10 Tbit/s QAM Quantum Noise Stream Cipher Coherent Transmission Over 160 km," J. Lightwave Technol., vol. 39, pp. 1056-1063, 2021. DOI: 10.1109/JLT.2020.3016693

[11] K. Tanizawa, and F. Futami, "Tradeoff between Reach and Security in Nyquist WDM Transmission of PSK Y-00 Quantum Stream Cipher," IEEE Photon. Technol. Lett., vol. 35, pp. 1147-1150, 2023.

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

[13] F. Futami, K. Tanizawa, and K. Kato, "Field-installed Fiber Transmission of Y-00 Quantum Stream Cipher with Quantum Deliberate Signal Randomization," Proc. SPIE 12429, Next-Generation Optical Communication: Components, Sub-Systems, and Systems XII, 124291J, 2023.

[14] 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 and Exhibition (OFC 2023), M2I.6, 2023.