ISSN 2186-6570

# Analysis of Eavesdropper's Correct Signal Detection Probability for BPSK Y-00 Quantum Stream Cipher with Deliberate Signal Randomization

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.12, No.1, 11-14, 2022

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.12 No.1 : 11−14 (2022)


# Analysis of Eavesdropper's Correct Signal Detection Probability for BPSK Y-00 Quantum Stream Cipher with Deliberate Signal Randomization

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*—The Y-00 quantum stream cipher (Y-00 cipher) is a direct data encryption system in which randomization techniques such as overlap selection keying, random basis selection, and irregular mapping are introduced for strong security. Deliberate signal randomization (DSR) is a keyless randomization method that enhanced the security of the Y-00 cipher system. This study analyzes the probability of correct signal detection by an eavesdropper for a binary phase-shift keying (BPSK) Y-00 cipher signal with DSR, assuming that DSR adds a uniform distribution of phase values to the BPSK signals. The probabilities of the Y-00 cipher measured using heterodyne detection were numerically calculated using the derived expression. The probability with a DSR index of 0.1 was approximately two orders of magnitude lower than that without DSR when the signal power was as high as 0 dBm.**

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

## I. Introduction

Sensitive data in communication systems should be protected from eavesdropping. The use of a cipher is promising for preserving communication data. The Y-00 quantum stream cipher protects data by randomizing multilevel modulated signal light using quantum noise [1-4]. An outstanding feature is that it guarantees security. In the Y-00 cipher, various randomization techniques [5] such as overlap selection keying (OSK), random basis selection, irregular mapping (IR), and deliberate signal randomization (DSR) are implemented for higher security. DSR is a keyless randomization technique that provides strong protection against attacks on data or keys during direct encryption using known text attacks [6-9]. DSR has the advantage of only needing additional functions to be included in the transmitter. However, it has a drawback in that it degrades the communication characteristics of the legitimate receiver. The bit error rate characteristics of a legitimate receiver were analyzed when DSR was added to the Y-00 cipher of the binary phase-shift keying (BPSK) signal [10]. In addition, the noise-masking amount, which represents the amount of randomization due to quantum noise, was analyzed. It has been found that it can be increased by several orders of magnitude [11]. The DSR dependence of the amount of noise masking was analyzed and showed that it can achieve large noise masking almost independently of the optical signal power, which increases the design freedom of fiber-optic communication systems using a Y-00 cipher. Furthermore, quantum DSR (QDSR) was experimentally demonstrated, in which DSR is driven by a random number generated from quantum noise. We have shown that QDSR provides flexibility in the design of Y-00 cipher communication systems [11].

In this study, the probability of an eavesdropper was analyzed correctly discriminating between Y-00 cipher signals and DSR. In the analysis, it was assumed that DSR adds a uniform distribution of phase values to the BPSK signals, and the signals have a Gaussian noise distribution. Subsequently, the derived expression was used to evaluate the probability numerically, and found that it was approximately two orders of magnitude smaller than that without DSR. In addition, it was found that the probability is almost independent of the power of the optical signals, which can make the design of Y-00 cipher optical fiber communication systems more flexible.

## II. Deliberate Signal Randomization

Figure 1 shows the operating principle of the Y-00 cipher with the BPSK data modulation. Data are encrypted by rotating the phase of the BPSK signal bit-by-bit, as shown in Fig.1 (a), where the DSR is not utilized. The rotation angle $\theta_h$ of BPSK is determined by a random basis selection based on a digital pseudo-random number (PRN) extended from the pre-shared short key, where $-\pi/2 \le \theta_h \le \pi/2$ and $-M \le h \le M$. The number of bases was $M$, and the order of the BPSK signal after encryption was $2M$. The adjacent phase difference was $\Delta\theta_{basis} = \pi/M$. It can be intuitively understood that noise prevents eavesdropping attempts from accurately detecting the high-order PSK (e.g., 32,768 PSK). In contrast, a legitimate receiver with a pre-shared key can detect the original BPSK signal by subtracting $\theta_h$ bit-by-bit. The masking effect is quantified by defining the masking number $\Gamma_{BPSK}$ as $\Gamma_{BPSK} = \Delta\phi/\Delta\theta_{basis}$ where $\Delta\phi$ is the amount of phase noise of the BPSK signals. The masking number $\Gamma_{BPSK}$ is inversely proportional to the square root of the optical power $P_S$ [12]. A higher power leads to a small $\Gamma_{BPSK}$, that is, poor security. This indicates that a Y-00 cipher communication system that uses higher optical power signals tends to be less secure.

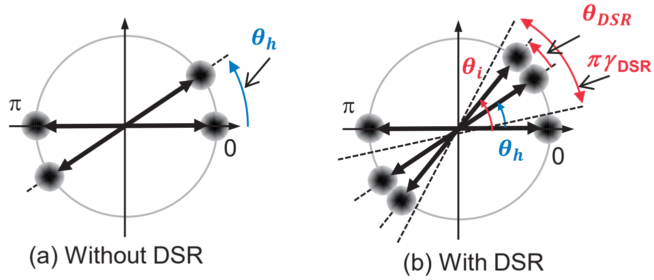


Fig. 1. Constellation of a BPSK signal (a) with random basis selection and no DSR and (b) with random basis selection and DSR

Figures 1(b) shows the constellation of a BPSK signal with the DSR. The phase $\theta_{DSR} = \theta_i - \theta_h$, which is determined by a random number, is added to the phase of the BPSK signal after the phase rotation of the random basis selection. $\theta_i$ is the phase of the BPSK signal after DSR. The range of the phase rotation with DSR is $\theta_{DSR} = \pi\gamma_{DSR}$ where the DSR index $\gamma_{DSR}$ represents the depth of randomization. The legitimate receiver does not share the DSR with the transmitter. Therefore, unlike the randomizations of OSK, random basis selection, and IR, the intended receiver cannot subtract the randomization of the DSR. The receiver sets the threshold to the y-axis after subtracting $\theta_h$ and then makes a binary decision. Because DSR is a keyless randomization, in which no key is required for the binary decision in the receiver, the receiver's digital signal processing is simplified. A drawback is that residual noise from the DSR remains, and the detection error caused by the noise degrades the BER of the legitimate receiver [10].

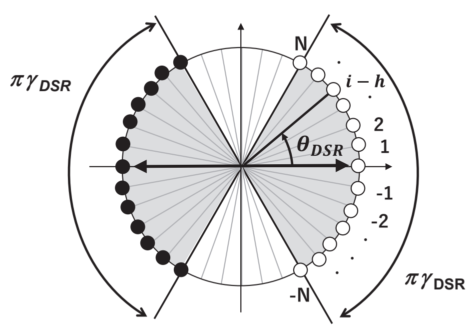


Fig. 2. Schematic of a constellation of BPSK signals to which various amounts of DSR are added

Figure 2 shows an example of DSR, with a constellation of BPSK signals overlaid with various amounts of DSR, where the phase of $\theta_h$ is subtracted for clarity. Phase $\theta_{DSR}$ was added to the phase of the BPSK signal after the phase rotation of $\theta_h$ where $\theta_{DSR} = \theta_h + \Delta\theta_{basis} \times (i-h)$ and $h - N \le i \le N + h$. Here, $2N+1$ represents the number of signal destinations by DSR. The DSR index was expressed as $\gamma_{DSR} = 2N/M$. For instance, the DSR number $N = M/2$ achieves full DSR and $\gamma_{DSR} = 1$. The noise-masking number for BPSK signals with DSR is defined as $\Gamma_{DSR} = (\Delta\phi_{shot} + \pi\gamma_{DSR})/\Delta\theta_{basis} = \Gamma_{BPSK} + \pi\gamma_{DSR}/\Delta\theta_{basis.}$ It should be noted that a higher masking number is achievable by merely increasing the DSR index. $\Gamma_{DSR}$ is almost independent of the optical signal power when $\Gamma_{BPSK} \ll \theta_{DSR}/\Delta\theta_{basis}$ while $\Gamma_{BPSK}$ is dependent on the optical power.

## III. Correct Signal Detection Probability of Eavesdropper

The correct signal detection probability of an eavesdropper was analyzed for a BPSK Y-00 cipher signal using DSR. Before examining the probability, the conditional probability density function of the measurement outcome for the *j*th signal of the M-ary PSK signals was discussed. As shown in Fig.3, it is assumed that the *j*th signal is correctly received when

$$\theta_j - \Delta < \theta \le \theta_j + \Delta \tag{1}$$

where $\theta_j$ is the phase of the *j*th PSK signal, and $\Delta = \pi/2M$.

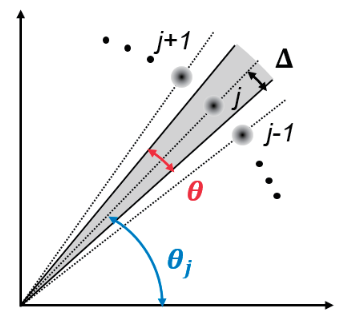


Fig. 3. M-ary PSK signals. The *j*th signal is correctly received when the signal is detected in the gray area.

Then, the conditional probability density function is derived in [13] as

$$p(\theta|i) \approx \frac{\cos[\theta-\theta_i]}{\sqrt{2\pi/\gamma}} \exp\left[-\frac{\sin^2[\theta-\theta_i]}{2/\gamma}\right] \tag{2}$$

where $\theta_i$ is the phase of the *i*th signal, and γ is the signal-to-noise ratio defined by $\gamma = A^2/\sigma^2$ where A and σ are the amplitude and noise of the signal, respectively. The approximation $\gamma \gg 1$ is used for the derivation. The probability that the *i*th signal is sent and the *j*th signal is received is expressed as follows:.

$$P_{Y|X}(j|i) = \int_{\theta_j-\Delta}^{\theta_j+\Delta} p(\theta|i)d\theta\,. \tag{3}$$

Substituting Eq.(2) into Eq.(3) leads to

$$P_{Y|X}(j|i) \approx \frac{1}{2}\left(erf\left[\sqrt{\frac{\gamma}{2}}\sin(\theta_j-\theta_i+\Delta)\right]\right.$$
$$\left.-erf\left[\sqrt{\frac{\gamma}{2}}\sin(\theta_j-\theta_i-\Delta)\right]\right). \tag{4}$$

Here, *j* and *i* satisfy the following relation

$$|\theta_j - \theta_i \pm \Delta| < \pi/2. \tag{5}$$

For other *j* and *i*, $P_{Y|X}(j|i) = 0$. In general, the relationship is as follows.

$$P_X(i)P_{Y|X}(j|i) = P_Y(j)P_{X|Y}(i|j). \tag{6}$$

Because the probability that a sender selects the *i*th signal is given by $P_X(i) = 1/2M$ and the probability that a receiver receives the *j*th signal is $P_Y(j) = 1/2M$, the following relation is given:

$$P_{X|Y}(i|j) = P_{Y|X}(j|i) \tag{7}$$

Next, the correct signal detection probability of an eavesdropper is discussed for the BPSK Y-00 signals with DSR. The sender selects the *h*th signal and then randomly selects the

$i$th signal from the 2N +1 candidates from $h$-$N$ and $h$+$N$. When the eavesdropper receives the $j$th signal, it reads the correct signal. The probability that the $i$th signal is selected from the $2N+1$ signals by the sender is

$$P_X(i) = \frac{1}{2N+1} \tag{8}$$

for $h$-$N \leq i \leq h$+$N$. For other $i$, $P_X(i) = 0$. The probability that an eavesdropper receives the $h$th signal correctly is

$$\begin{aligned} P_{EVE} &= \sum_{i=h-N}^{h+N} P_X(i) P_{X|Y}(j = h|i) \\ &= \frac{1}{2N+1} \sum_{i=h-N}^{h+N} P_{Y|X}(j = h|i)\,. \end{aligned} \tag{9}$$

From Eqs. (4) and (9), $P_{EVE}$ is given by

$$P_{EVE} = \frac{1}{2N+1} erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(\frac{2N+1}{2M/\pi}\right)\right] \tag{10}$$

With the condition of $(2N+1)\pi/2M \ll 1$, it is further simplified as

$$P_{EVE} = \frac{1}{2N+1} erf\left(\frac{2N+1}{\sqrt{2}\Gamma_{BPSK}}\right) \tag{11}$$

## IV. Numerical Calculation

The probability *of a* $P_{EVE}$ was calculated using the derived expressions. Figure 4 shows the probability $P_{EVE}$ for DSR number $N$ when the masking numbers are $\Gamma_{BPSK}$ = 10, 50, 100, and 200. When the DSR number is increased, the probability of each $\Gamma_{BPSK}$ is almost constant and the same for $1/\Gamma_{BPSK}$ until the DSR number is comparable to $\Gamma_{BPSK}$. The DSR number was further increased, and the probability decreased and converged to the same probability for all $\Gamma_{BPSK}$ values.

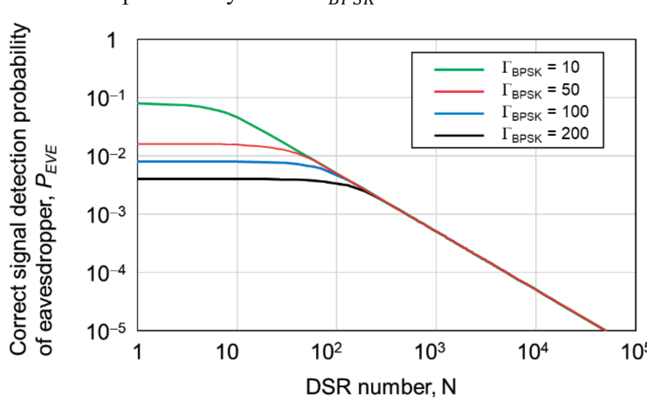


Fig. 4. The correct signal detection probability of BPSK signals with DSR.

Next, the probability $P_{EVE}$ for an optical signal power $P_S$ with a data rate of 10 Gb/s, a wavelength of 1.55 μm and the basis number of M = 32,768 was calculated with the DSR index of $\gamma_{DSR} = 0.1$. Here, masking with quantum noise is considered only, and the optical signal power is calculated using Eq. (1) [12]. The probabilities are plotted in Fig. 5 as a solid line. For comparison, the probabilities without DSR are plotted with dashed lines. Without DSR, the probability decreases at lower powers. For instance, the probabilities with $P_S$ = 0 and –20 dBm are 0.05 and 0.005, respectively, which shows that the security with higher powers is lower than that with lower powers, and the security of an optical communication system is dependent on the optical signal power. In contrast, the probability with DSR is independent of the optical signal power. In addition, the probability was lower than that without DSR. For instance, the probability $P_{EVE}$ for $P_S$ = 0 dBm is two orders of magnitude smaller, and the probability $P_{EVE}$ even for $P_S$ = –20 dBm is more than an order of magnitude smaller.

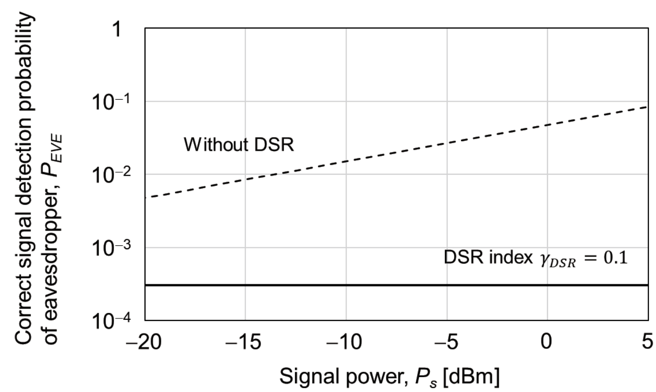


Fig. 5. The correct signal detection probability of 10-Gb/s BPSK Y-00 signals with the basis number of M = 32,768 and the DSR index of $\gamma_{DSR} = 0.1$.

## V. Summary

We derived an expression for the correct signal detection probability of an eavesdropper for the BPSK Y-00 cipher signals with DSR, assuming that DSR adds a uniform distribution of phase values to the BPSK signals. Subsequently, the probability of the Y-00 cipher being measured using heterodyne detection was numerically calculated. The probability for 10-Gb/s signals at a wavelength of 1.55 μm with a basis number of $2^{15}$ and an optical power of 0 dBm was approximately two orders of magnitude lower than that without DSR when the DSR index was 0.1. This probability can be further decreased by increasing the DSR index. The optical signal power does not affect the probability, which can provide flexibility in the system design of optical fiber communications.

## VI. Acknowledgement

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

## References


[1] H. P. Yuen, "KCQ: A new approach to quantum cryptography I. General principles and qumode key generation," quant-ph/0311061, 2004.

[2] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," *Phys. Rev. Lett.*, vol.22, 227901, 2003.

[3] 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*, 72, 022335, 2005.

[4] K. Kato and O. Hirota, "Quantum quadrature amplitude modulation system and its applicability to coherent state quantum cryptography," SPIE conference on quantum communication and imaging III. SPIE Proc. vol-5893, 2005.

[5] K. Kato, O. Hirota, "Quantum stream cipher Part IV: Effects of the deliberate signal randomization and the deliberate error randomization," Proc. SPIE 6305, Quantum Communications and Quantum Imaging IV, 630508, 2006.

[6] 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, 2005.

[7] T. S. Usuda, "Y-00 key generation with non-weak coherent states –Effect of DSR on Eve's and Bob's error performance–," Symposium on quantum cryptography by optical communications, Tamagawa University/Chuo University, Tokyo, Japan, Nov.28-29, 2005.

[8] O. Hirota, K. Kato, M. Sohma, T. S. Usuda, K. Harasawa, "Quantum stream cipher based on optical communications," Proc. SPIE 5551, Quantum Communications and Quantum Imaging II, 2004.

[9] O. Hirota and K. Kurosawa, "Immunity against Correlation Attack on Quantum Stream Cipher by Yuen 2000 Protocol," Quantum Information Processing, Vol. 6, No. 2, pp.81-90, April 20

[10] F. Futami, K. Tanizawa, K.Kato, "Bit Error Ratio Analysis of Legitimate Receiver for BPSK Y-00 Quantum Stream Cipher Signals with Deliberate Signal Randomization," Tamagawa University Quantum ICT Research Institute Bulletin, Vol.11, No.1, 19-21, 2021.

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

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

[13] K. Kato, “A Note on the Error Probability by Homodyne Receiver for M-ary PSK Coherent State Signal via Optical Transmission Lines with Amplifiers,” Tamagawa University Quantum ICT Research Institute Bulletin, Vol.9, No.1, 33-39, 2019.


## Appendix

Eq.(10) is derived from Eqs. (4) and (9) in the following way. First, substituting Eq.(4) into Eq.(9) leads to

$$P_{EVE} = \frac{1}{2(2N+1)} \sum_{i=h-N}^{h+N} \left( erf\left[\sqrt{\frac{\gamma}{2}} \sin(\theta_h - \theta_i + \Delta)\right] - erf\left[\sqrt{\frac{\gamma}{2}} \sin(\theta_h - \theta_i - \Delta)\right] \right) \quad (12)$$

Next, $\theta_h = 2h\pi/2M$, $\theta_i = 2i\pi/2M$ and $\Delta = \pi/2M$ are substituted into Eq.(12) and

$$P_{EVE} = \frac{1}{2(2N+1)} \sum_{i=h-N}^{h+N} \left( erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(\frac{2(h-i)+1}{2M/\pi}\right)\right] - erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(\frac{2(h-i)-1}{2M/\pi}\right)\right] \right) \quad (13)$$

is obtained. Here, $i$ is replaced with $j = i - h$. Then $P_{EVE}$ is given by

$$P_{EVE} = \frac{1}{2(2N+1)} \sum_{j=-N}^{N} \left( erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(\frac{-2j+1}{2M/\pi}\right)\right] - erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(\frac{-2j-1}{2M/\pi}\right)\right] \right). \quad (14)$$

Eq.(14) is simplified into

$$P_{EVE} = \frac{1}{2(2N+1)} \left( erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(\frac{2N+1}{2M/\pi}\right)\right] - erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(-\frac{2N+1}{2M/\pi}\right)\right] \right). \quad (15)$$

Using the relationship of $erf(-X) = -erf(X)$, Eq.(15) is further simplified into

$$P_{EVE} = \frac{1}{2N+1} erf\left[\sqrt{\frac{\gamma}{2}} \sin\left(\frac{2N+1}{2M/\pi}\right)\right]. \quad (10)$$