ISSN 2186-6570

Bit Error Ratio Analysis of Legitimate Receiver for BPSK Y-00 Quantum Stream Cipher Signals 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.11, No.1, 19-21, 2021

Bit Error Ratio Analysis of Legitimate Receiver for BPSK Y-00 Quantum Stream Cipher Signals 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 for achieving a secure Y-00 cipher system. In this study, a closed-form expression of the bit error ratio (BER) of a legitimate receiver for binary phase-shift keying (BPSK) Y-00 cipher signals with DSR was derived assuming that DSR adds a uniform distribution of phase values to the BPSK signals. Using the derived expression, the BERs of the Y-00 cipher measured with homodyne detection were numerically calculated. The BER was approximately two orders of magnitude lower than 0.5, when the DSR index was 100%, the number of bases was 2^{11}, and the number of photons was 10,000, showing that full DSR is possible.**

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

I. Introduction

The Y-00 quantum stream cipher achieves security by masking the cipher signal with quantum noise [1-4]. Various randomization techniques have been used to enhance security [5]. Randomization techniques, such as overlap selection keying (OSK), random basis selection, and irregular mapping (IM), have been implemented in our Y-00 quantum stream cipher transceiver, and both strong security and high communication performance have been achieved. Deliberate signal randomization (DSR) is a type of keyless randomization technique that can provide strong security against attacks on data or keys in direct encryption using known text attacks [6-9]. Its implementation is easy owing to the keyless randomization. However, it has a disadvantage in that it increases bit errors even for a legitimate receiver because noise from DSR remains. To date, no closed-form expression of bit error ratio (BER) with DSR has been reported, although a numerical analysis result of such errors measured with heterodyne detection has been reported [6].

In this study, we derive a close-form expression to show the BER of legitimate receivers for Y-00 cipher signals composed of binary phase-shift keying (BPSK) signals with DSR in the case of a ciphertext-only attack under the assumption that DSR adds a uniform distribution of phase values to the BPSK signals. Subsequently, we use the derived expression to evaluate the BER characteristics of the legitimate receiver measured with homodyne detection.

II. Deliberate Signal Randomization

Figure 1 briefly illustrates the operating principle of the Y-00 cipher. For details, please refer to the references [1,2]. The transmitter and intended receiver share the common key, pseudo-random number generator (PRNG), and randomizations of OSK and IM before their cipher communication starts. A block of pseudo-random numbers extended by using the PRNG with the common key is used to select a basis for scrambling the data after OSK, and the data are mapped through the basis and IM. In this process, a BPSK signal carrying the data is converted into a cipher signal composed of a multilevel phase modulation signal with the phase values of 2M, where M is the number of bases. As the number of bases increases, the cipher signal is masked by quantum (shot) noise, which is inevitable at detection. Such masking disables the eavesdropper’s correct discrimination of the cipher signals, thus achieving security. The intended receiver can subtract out the randomizations added to the signal at the transmitter, leaving a simple binary decision on the data bit to recover the original data.

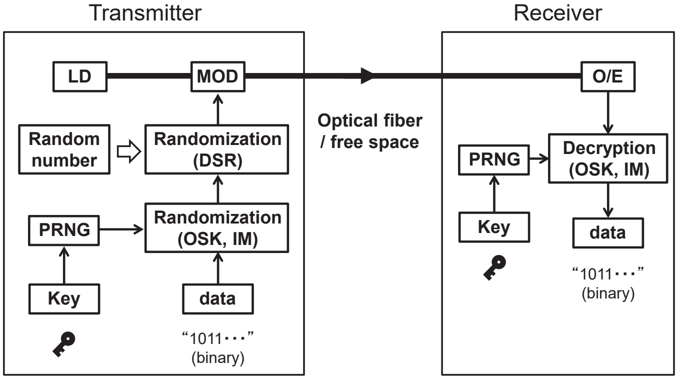
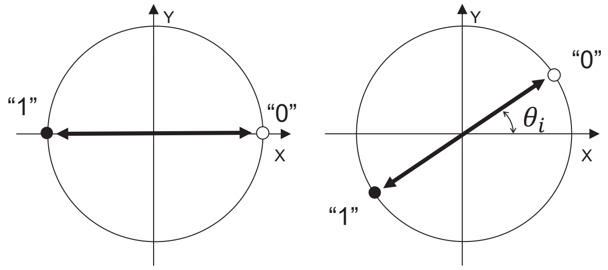


Fig. 1. Schematic of a cipher communication system where DSR driven by random numbers is added in the transmitter

In addition to these randomizations of OSK, random basis selection, and IM, DSR further randomizes the signal using a random number, as shown in Fig. 1, and adds another complexity to enhance the security of the Y-00 cipher system. DSR can be added to a signal either digitally using a fast random-number generator or analogously using a noise-based random number.

Figures 2(a) and 2(b) show the constellations of a BPSK signal without and with DSR, respectively, to illustrate the principle of DSR. The phase of the BPSK signal is rotated by the amount of DSR, θ_i, determined by a random number. The legitimate receiver does not share the DSR with the transmitter. Therefore, unlike in the previous randomizations of OSK, random basis selection, and IM, the intended receiver cannot subtract out the randomization of DSR. The receiver sets the threshold to the y-axis and then makes a binary decision. As DSR is a keyless randomization, where no key is required for the binary decision in the receiver, the receiver's digital signal processing is apparently simplified. A drawback is that residual noise from DSR remains, and the detection error caused by the noise degrades the BER of the legitimate receiver.



(a) With no DSR (b) With DSR

Fig. 2. Constellation of a BPSK signal (a) with no DSR and (b) with DSR

Figure 3 shows an example of digital DSR, showing a constellation of BPSK signals overlaid with various amounts of DSR. A BPSK signal is mapped onto the Y-00 cipher. The phase of the BPSK signal with DSR ranges from $-\theta_N/2$ to $+\theta_N/2$, where $\theta_N = \pi N/M$ and N is an integer ($0 \le N \le M/2-1$). The DSR index was defined as $m_{DSR} = 2N/(M-2)$. For instance, $N = M/2 - 1$ achieves full DSR with $m_{DSR} = 1$.

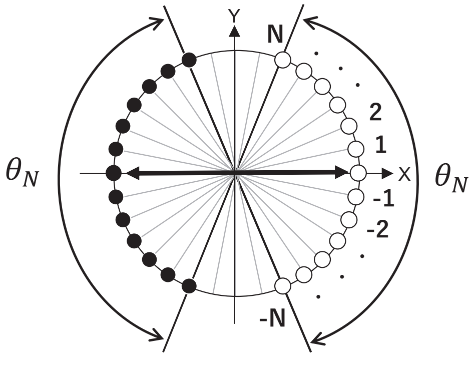


Fig. 3. Schematic of a constellation of BPSK signals to which various amounts of DSR are added

III. BER of Legitimate Receiver for BPSK Y-00 Cipher

The BER of the Y-00 cipher signals with DSR for a legitimate receiver was analyzed. We assumed that the basis is composed of BPSK signals, and the signals are measured with homodyne or heterodyne detection. We also assumed a uniform probability distribution of phase values with the addition of DSR.

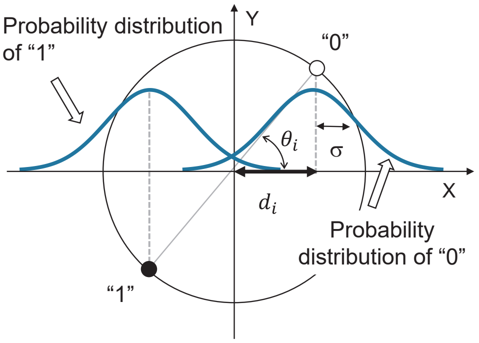

Probability distribution of "1"
Y
"0"
θ_i
σ
X
d_i
Probability distribution of "0"
"1"

Fig. 4. Model showing the measurement result of a BPSK signal after DSR at the legitimate receiver

Figure 4 shows a BPSK signal with DSR and the probability distributions of data "0" and "1." In the analysis, we observed the projection of the probability distribution onto the x-axis. The x-axis corresponds to the basis before DSR is added. Let v denote the measurement outcome of the legitimate receiver. When the i-th data of "0" with a phase value of θ_i ($-N \le i \le +N$) is sent from the transmitter, the probability density function of the measurement result v at the legitimate receiver is expressed as

$$f(x|i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-d_i)^2}{2\sigma^2}\right). \tag{1}$$

Here, d_i is expressed as $d_i = \sqrt{n_S}\cos(i\pi/M)$, where n_S is the number of photons. The average error probability is expressed using Eq. (1) as

$$P_0^B = \frac{1}{2N+1} \sum_{i=-N}^{N} \int_{-\infty}^{0} f(x|i)\, dx. \tag{2}$$

Substituting Eq. (1) into Eq. (2) and rearranging it, we obtain

$$P_0^B = \frac{1}{2(2N+1)} \sum_{i=-N}^{N} erfc\left(\frac{d_i}{\sqrt{2}\sigma}\right), \tag{3}$$

where $erfc()$ is the complementary error function. The probability of error in observing data "1" as data "0" is expressed as follows:

$$P_1^B = \frac{1}{2N+1} \sum_{i=-N}^{N} \int_{0}^{+\infty} f(x|i)\, dx. \tag{4}$$

This leads to

$$P_1^B = \frac{1}{2(2N+1)} \sum_{i=-N}^{N} erfc\left(\frac{d_i}{\sqrt{2}\sigma}\right). \tag{5}$$

Assuming that the probabilities of data "1" and "0" are the same, the following closed-form expression of the BER of the legitimate receiver is obtained.

$$\begin{aligned} BER &= \frac{1}{2}P_0^B + \frac{1}{2}P_1^B \\ &= \frac{1}{2(2N+1)}\sum_{i=-N}^{N} erfc\left(\frac{d_i}{\sqrt{2}\sigma}\right). \end{aligned} \tag{6}$$

IV. Numerical Calculation of BER

The BERs were calculated using the derived expression. A variance of σ = 1/2 for homodyne detection was employed. Figure 5 shows the BERs for the average numbers of photons when the DSR index is set to 90% (m_{DSR} = 0.9) and M = 2^{11}. Although the DSR index was high, a BER of 10^{-5} was achieved for BPSK Y-00 signals with 100 photons per bit. Signals with 300 or more photons per bit achieved BERs lower than 10^{-9}.

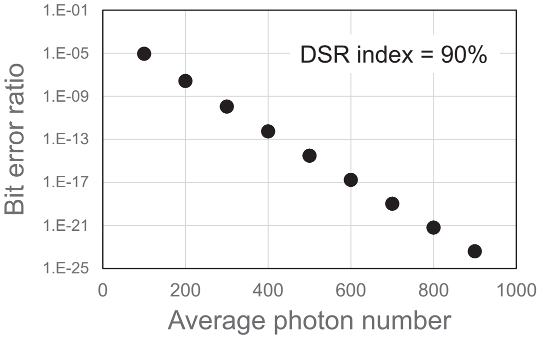


Fig. 5. BER of BPSK signals with DSR at the legitimate receiver for average photon numbers

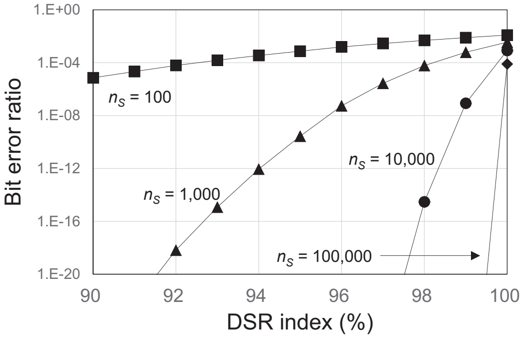


Fig. 6. BER of BPSK signals at the legitimate receiver versus the DSR index for photon numbers

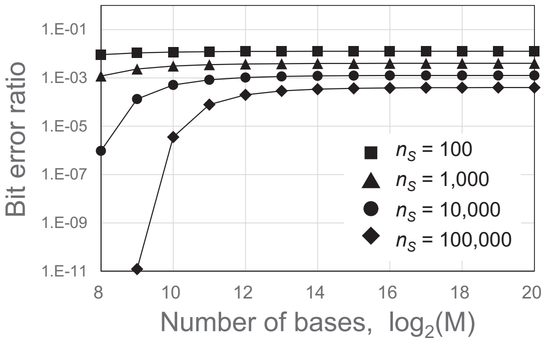


Fig. 7. BER of BPSK signals with full DSR at the legitimate receiver versus the number of bases for photon numbers

Subsequently, the BERs of photons per bit of 100, 1,000, 10,000, and 100,000 are plotted in Fig. 6 when the DSR index is changed from 85% to 100%. The photon numbers correspond to the optical powers of -47, -37, -27, and -17 dBm, respectively, for a symbol rate of 10 Gbaud. The BER increased as the DSR index increased. BERs with a DSR index of 100% for all photon numbers were much lower than 0.5, indicating that full DSR is possible. Finally, the BERs are plotted as a function of the number of bases for various photon numbers. As the number of bases increased, the BER converged to a constant value. The value decreased as the number of photons increased. For a photon number of 10,000, the BER was 1.3×10^{-3}. As the number of bases decreased, the BER tended to be smaller. This is because the shot noise was relatively lower than the distance between adjacent signals when the number of bases decreased.

V. Summary

We derived a closed-form expression for the BER of legitimate receivers for BPSK Y-00 cipher signals with DSR, assuming that DSR adds a uniform distribution of phase values to the BPSK signals. Subsequently, the BERs of the Y-00 cipher measured with homodyne detection were numerically calculated using the derived expression. The BER was approximately two orders of magnitude lower than 0.5, when the DSR index was 100%, the number of bases was 2^{11}, and the number of photons was 10,000, showing that full DSR is possible. In the future, the BER for an eavesdropper will be analyzed using heterodyne detection.

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 2007.