Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications

Fumio Futami, *Member, IEEE*, Ken Tanizawa, *Member, IEEE*, and Kentaro Kato, *Member, IEEE*

(Invited Paper)

***Abstract*—The Internet plays an essential role in modern societies and in the amount of sensitive data transported over the optical networks that shows its' importance has increased drastically. Therefore, it is critical to develop data protection schemes for optical fiber communications to provide user security. The Y-00 quantum-noise randomized stream cipher that employs extremely high-order modulation and restricts an attacker's interception of ciphertext is a practical candidate for providing data protection. In this article, we introduce the operation principle of the Y-00 cipher with respect to data encryption and decryption. The Y-00 cipher combines the mathematical encryption of multi-level signaling and physical randomness, and provides a high level of security to the physical layer of optical communications and a high communication performance. We also present the noise masking phenomenon of the Y-00 cipher with intensity modulation (IM). This noise masking is generated by shot noise, i.e., quantum noise and additive noise such as amplified spontaneous emission noise. The noise masking phenomenon fails an attacker's interception of the ciphertext. The secrecy of the IM Y-00 cipher is also discussed, and an approximate analytical solution is introduced for evaluating the probability of the attackers accurately guessing the ciphertext. Finally, the secrecy of a 1,000-km transmission system is experimentally demonstrated with the Y-00 cipher transceiver at data rate of 1.5-Gb/s using the derived analytical solution to deduce the high secrecy of the entire transmission system.**

***Index Terms*—Communication system security, encryption, modulation, optical fiber communication.**

I. Introduction

SENSITIVE data, such as confidential and personal information, are stored and communicated in the Internet. Therefore, access to such information by unauthorized parties must be restricted. A networking framework is defined by the open systems interconnection model to implement protocols in seven layers. It is essential to make all these layers secure for building a secure network. The classical cipher based on mathematical theories is employed for the sensitive data, when required. The binary digital signals of the data are processed in the classical cipher to provide binary digital signals of the ciphertext, which can be easily intercepted and possibly moved into cryptanalysis by the attackers. While the data must be processed digitally from layer 2 or higher, various modulation schemes and physical phenomena can be applied for encryption in layer 1 of the physical layer to provide secure communication systems. A cipher communication system includes a key and a cipher for ciphering plaintext and deciphering ciphertext at both ends of a transmission link (Fig. 1). Therefore, the development of a secure key distribution scheme and the invention of strong algorithms for data encryption and decryption are necessary to realize secure communication. In the classical cipher, RSA (Rivest–Shamir–Adleman) algorithm is a practically utilized scheme for key distribution. A post-quantum cryptosystem has been studied for secure key distribution against attack by a quantum computer. As for the data encryption scheme, the advanced encryption standard (AES) is practically used. One-time pads (OTPs) are information-theoretically secure when a truly random cryptographic key is given, although they are hardly cost effective. Key distribution is achieved using physical phenomena. For instance, BB84 is a well-known protocol that uses quantum key distribution (QKD) based on quantum entanglement [1]. Data encryption using physical phenomena is also possible. For instance, secure systems, such as the ones assisted by chaos [2], based on optical code domain multiplexing [3], or assisted by multi-level signaling with physical randomness of noise [4], have been reported. Any combination of a key distribution scheme and a data encryption scheme provides a cipher communication system. The integrity of the key is an important issue that is overcome by using a third party known

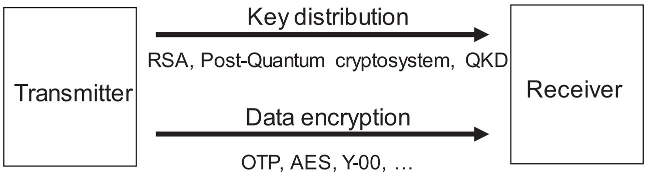


Fig. 1. A cipher communication system generally requires a cryptographic key and a cipher for data encryption and decryption.

Manuscript received November 14, 2019; revised February 4, 2020 and March 18, 2020; accepted March 24, 2020. Date of publication April 10, 2020; date of current version May 15, 2020. This work was supported by JSPS KAKENHI under Grant JP19K04397 and Grant JP18K04290. *(Corresponding author: Fumio Futami.)*

The authors are with Tamagawa University, Tokyo 194-8610, Japan (e-mail: futami@lab.tamagawa.ac.jp; tanizawa@lab.tamagawa.ac.jp; kkatop@lab.tamagawa.ac.jp).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2020.2985709

as certificate authority (CA), which certifies the key ownership. We focused on a data encryption scheme assisted by multi-level signaling because we aim to develop a data encryption scheme that realizes practical and secure communication systems with a high data rate of more than 1 Gbit/s and a long transmission distance of over 1000 km. We assumed herein that the same cryptographic keys used for encryption at the transmitter end and decryption at the receiver end are shared securely in advance before the cipher communication starts. In addition, we aim to achieve a high compatibility with the deployed optical communication infrastructure for practical applications. As introduced in the subsequent section, the Y-00 quantum-noise randomized stream cipher (Y-00 cipher) [4], originally proposed to utilize masking using quantum noise, employs multi-level signaling with extremely high-order modulation and hides the ciphertext by imposing noise on cipher signals. This feature is remarkably different from that of the classical cipher, as the Y-00 cipher forces an attacker to fail the interception of the ciphertext.

In this paper, we extend the presented paper in [5] and discuss further on Y-00 cipher encryption and decryption principles using Y-00 cipher with intensity modulation (IM). In addition, we discuss the noise masking generated from the shot noise, i.e., quantum noise and additive noise, and then compare the amounts of the noise masking obtained using typical parameters in practical Y-00 cipher communication systems. We then introduce an approximate analytical solution for evaluating the probability of guessing the accurate ciphertext expressed with noise masking numbers. Using the probability, we evaluate the secrecy of a 1,000-km Y-00 cipher transmission system and experimentally demonstrate it using 1.5-Gb/s Y-00 cipher transceivers. It should be noted that we mainly focus on the IM Y-00 cipher in this study, although Y-00 cipher can also be realized by phase modulation (PM) and quadrature-amplitude modulation (QAM).

The reminder of this paper is organized as follows: the concept, features, and the basic operation principle of the Y-00 cipher is described in detail in section II. Then the noise masking achieved by shot noise and additive noise is presented in section III. An approximated analytical solution related to the probability of guessing the ciphertext accurately is introduced in section IV. The secrecy of the experimentally demonstrated transmission system is evaluated in section V, and the conclusions are presented in section VI.

II. Y-00 Quantum Stream Cipher

A. Concept and Features

A physical cipher that employs multi-level signaling and realizes a direct data encryption system is theoretically proposed [4] and experimentally demonstrated [6]. The realization scheme used for the cipher is called AlphaEta ($\alpha\eta$) or Y-00 quantum stream cipher. The Y-00 cipher utilizes both a mathematical cipher of the classical cryptosystem and the physical randomness of noise for achieving high security. The implementation of the Y-00 cipher include PM [7], IM [8], and QAM [9]. The data rates of experimental demonstrations [10]–[26] are in the Gb/s regime. The notion of the data encryption performed is illustrated in Fig. 2. The eye-diagram of the plaintext with binary signals is encrypted with multi-level signaling, and the eye-diagram of Y-00 cipher signals is closed. Therefore, even though an attacker can tap a portion of the Y-00 cipher signals, the interception of the ciphertext fails.

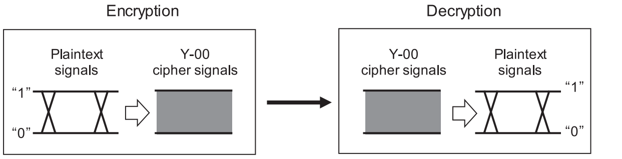


Fig. 2. Basic concept of theY-00 cipher that restricts the interception of ciphertext (Y-00 cipher signals) by an attacker.

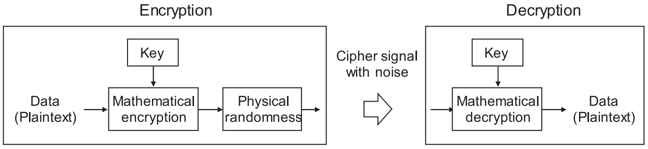


Fig. 3. Y-00 cipher direct data encryption system.

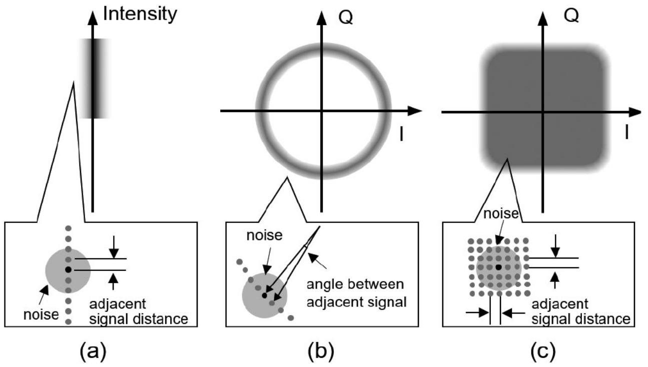


Fig. 4. Schematic of noise masking of (a) intensity modulation, (b) phase modulation, and (c) quadrature-amplitude modulation. Each inset shows the noise masking effect.

The Y-00 cipher is a symmetric key encryption scheme, where the same key is shared in advance with the transmitter and receiver for direct data encryption (Fig. 3). During the encryption, the physical randomness of the noise is combined with the mathematical encryption of multi-level signaling for hiding the ciphertext using the noise of Y-00 cipher signals. A legitimate receiver can recover the original signal of plaintext from the cipher signal masked with noise using a shared key and mathematical signal processing. The classical light from a laser diode enables the cipher signal transmission to the legitimate receiver.

B. Noise Masking for Restricting the Interception of Ciphertext

A cipher signal masked with noise is generated by multi-level signaling or high-order modulation. As the modulation order increases, the power difference between adjacent signals decreases. When the modulation order is significantly high, and the power difference is significantly low, a cipher signal is covered with the noise of the adjacent cipher signals [27]. Figs. 4(a), 4(b),

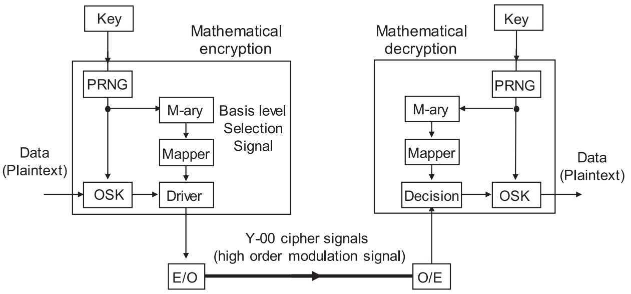
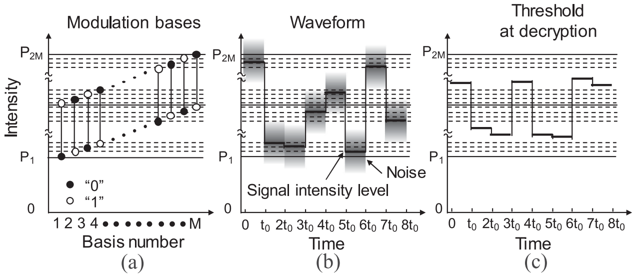


Fig. 5. Basic configuration of Y-00 cipher communication system (OSK - overlap selection keying).



Basis / Data	B_1	B_2	B_3	• • •	B_{M-2}	B_{M-1}	B_M
"0"	P_1	P_{M+2}	P_3	• • •	P_{M-2}	P_{2M-1}	P_M
"1"	P_{M+1}	P_2	P_{M+3}	• • •	P_{2M-2}	P_{M-1}	P_{2M}

(d)

Basis	B_1	B_2	B_3	• • •	B_{M-2}	B_{M-1}	B_M
Threshold	$\frac{P_1+P_{M+1}}{2}$	$\frac{P_2+P_{M+2}}{2}$	$\frac{P_3+P_{M+3}}{2}$	• • •	$\frac{P_{M-2}+P_{2M-2}}{2}$	$\frac{P_{M-1}+P_{2M-1}}{2}$	$\frac{P_M+P_{2M}}{2}$

(e)

Fig. 6. (a) A set of basis, (b) a waveform of IM with noise after encryption, and (c) threshold at encryption. Reference tables of (d) encryption and (e) decryption.

and 4(c) illustrate the noise masking in IM, PM, and QAM, respectively. The noise of the cipher signal (shown by gray circles in each inset) penetrates into adjacent signals. The noise includes the shot noise (quantum noise) and the additive noise of amplified spontaneous emission (ASE) noise.

The randomness of the quantum noise generated from the signal measurement is important in the theoretical investigation of the Y-00 cipher security in cryptography [28]. True randomness leads to unchanged secrecy. Therefore, masking the signal with a quantum noise provides high secrecy and is more robust against attackers. Accordingly, this cipher is called the "quantum"-noise randomized stream cipher. The ASE noise is usually dominant when the Y-00 cipher communication system is used in a long-haul link using optical amplifiers. The ASE noise is different from the shot noise because it is an additive noise. Although such a difference might lead to difference secrecy in cryptographic investigation, the noise masking by the ASE–signal beat noise also positively contributes to the restriction of the interception by an attacker. The security requirements for the mathematical encryption are mitigated because of the noise masking, which is a practical advantage compared to classical cryptography utilizing only mathematical encryption.

C. Basic Operation Principle

The basic operating principle of Y-00 cipher is introduced with reference to the typical configuration of Y-00 cipher shown in Fig. 5. The sets of modulation basis are defined in advance. Each basis comprises levels that encode plaintext. For example, a basis can include two levels of "0" and "1" in IM Y-00, as shown in Fig. 6(a), in which the number of bases is M. During encryption, a basis, B_i ($1 \leq i \leq M$), is selected in a bit-by-bit manner using a pseudo-random number generator (PRNG), which expands the pre-shared key into a much longer running key. The intensity level, P_i ($1 \leq i \leq 2M$), is selected by the basis and the incoming data of the plaintext by referring to the table of the basis for encryption (shown in Fig. 6(d)). The details of the randomization technique of overlap selection keying (OSK) and a mapper incorporated in the mathematical processing for higher security are provided in [28]–[33]. Fig. 6(b) shows the resulting time waveform of the high-order IM. An electrical digital-to-analog converter (DAC) is incorporated into the driver for E/O conversion. The number of bases M is practically limited by the resolution of the DAC, which is 12 bits at most for the speed of Gbaud. An optical multiplexing scheme using multiple electrical DACs for breaking the limit has been demonstrated earlier [23], [24], [26]. In decryption, a legitimate user uses the same PRNG, sets of bases, and the pre-shared key. Therefore, the adjacent signals need not be resolved for decryption. The threshold of the decision circuit is set in a bit-by-bit manner, as shown in Fig. 6(c), to the middle of two intensity levels of the basis ($(P_i + P_{M+i})/2$ for B_i) by referring to the table for decryption shown in Fig. 6(e), which results in recovering the original signal of plaintext. Given that the two levels within each basis are far from each other, correct decisions without errors can be achieved between legitimate users even in the presence of noise, as shown in Fig. 6(b).

D. Practical Applications

As the Y-00 cipher features a high connectivity with deployed optical communication, it can be used in several practical applications. A point-to-point transmission is an application. For instance, a long reach of over 1,000 km is demonstrated using inline repeater optical amplifiers [25]. The short reach of the cost-effective system includes another point-to-point transmission application, in which the current of a distributed feedback laser is directly modulated for compact transmitter, and no inline optical amplifier is employed over the 80 km transmission [14]. Other practical applications include the wavelength-division multiplexed transmissions [13], [16], overlay transmissions with non-cipher signals [7], [21], digital-coherent transmission of PM Y-00 cipher [24], [26] and QAM Y-00 cipher [15], [20], optical routing [22], and a free-space communication for secure optical wireless communications [17].

III. Noise Masking of the IM Y-00 Cipher

This section discusses the noise masking produced by the noise, which is the quantum noise (i.e., shot noise) and additive noise of the ASE noise. The amounts of noise masking by the shot noise and ASE noise are compared, and their effects to security are discussed.

A. *Noise Masking by Shot Noise*

Here, the noise masking phenomenon produced by the quantum noise is discussed, where quantum noise implies the shot noise. Multi-level IM signals denoted by $\mathrm{P_i}$ ($1 \leq \mathrm{i} \leq 2\mathrm{M}$) is considered, in which the numbers of intensity levels and bases are 2M and M, respectively. The signals have the same intensity difference. The maximum and minimum powers are $\mathrm{P_{2M}}$ and $\mathrm{P_1}$, respectively. The shot noise of the optical light with an optical power of P_0 detected by an ideal photodetector (PD) is represented as

$$\sigma_{shot} = e\sqrt{2P_0B/h\nu_0}, \qquad (1)$$

where *h* is the Planck constant, ν_0 is the optical light frequency, *e* is the electric charge, and *B* is the signal bandwidth. A responsivity of a PD in the analysis is assumed to be 1. The power difference of neighboring signal levels is derived as follows:

$$\Delta\mathrm{P}_{basis} = \frac{P_{2M}-P_1}{2M-1} \qquad (2)$$

Assuming that an ideal PD is utilized for optical-to-electrical conversion, the amount of noise masking is defined using shot noise and minimum power difference as follows:

$$\Gamma_{IM\_shot} = \frac{2\sigma_{shot}}{\Delta P_{basis}} = \frac{2(2M-1)e}{P_{2M}-P_1}\sqrt{\frac{2BP_0}{h\nu_0}} \qquad (3)$$

The noise masking number of the IM Y-00 cipher is related to parameters, such as the number of bases, signal frequency, signal bandwidth, and the maximum and minimum signal powers. The maximum power level of $\mathrm{P_0} = \mathrm{P_{2M}}$ demonstrates the highest $\Gamma_{\mathrm{IM\_shot}}$, and the minimum power level of $\mathrm{P_0} = \mathrm{P_1}$ demonstrates the lowest $\Gamma_{\mathrm{IM\_shot}}$. For avoiding $\Gamma_{\mathrm{IM}} = 0$, a DC offset of $\mathrm{P_1}$ ($\neq 0$) is intentionally added in IM Y-00 at the expense of the transmission performance of Y-00 cipher. By substituting the ratio of the maximum power to minimum power, $\mathrm{r} = \mathrm{P_{2M}} / \mathrm{P_1}$, and $\mathrm{P_0} = \mathrm{P_M} = (\mathrm{P_{2M}} + \mathrm{P_1})/2$ in (3), we obtain

$$\Gamma_{IM\_shot} = \frac{(2M-1)(r+1)e}{r-1}\sqrt{\frac{2B}{P_M h\nu_0}} \qquad (4)$$

The masking number approaches infinity, as *r* approaches 1 ($\mathrm{P_{2M}} = \mathrm{P_1}$), and the Y-00 cipher transmission performance degrades. Meanwhile, the transmission performance is better when *r* is large. However, the masking number of $\mathrm{P_1}$ becomes much smaller than that of $\mathrm{P_{2M}}$. We set the max-to-min power ratio $\mathrm{r} = 2$ in the subsequent discussion and experiments to balance the transmission and security performances. The noise masking number is numerically calculated using (3), when the average signal power and number of bases are changed. In the calculation, the wavelength of the signal is set to $\lambda = 1550$ nm, which corresponds to $\nu_0 = 193.4$ THz. The signal bandwidth is denoted as $\mathrm{B} = 1.5$ GHz. Fig. 7 shows the noise masking numbers for $\mathrm{M} = 2^{11}$, 2^{13}, and 2^{15}, when the average power is changed from $-20 - 10$ dBm. Although an electrical DAC that achieves $\mathrm{M} = 2^{11}$ is employed in the following experiment, a higher M can be achieved using multiple electrical DACs [23]. The solid curves and dashed curves show the numbers of the minimum power ($\mathrm{P_1}$) and maximum power ($\mathrm{P_{2M}}$), respectively. These results indicate that lower power values and higher number of bases are preferred for realizing high noise masking numbers.

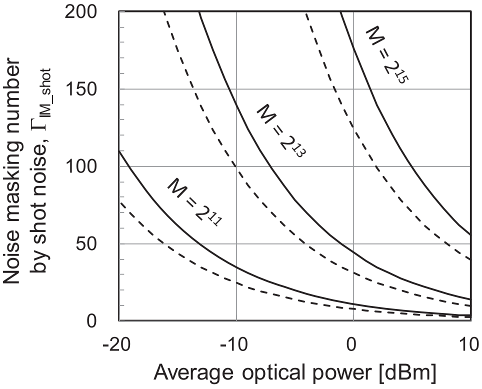


Fig. 7. Noise masking number by shot noise of the IM Y-00 cipher as a function of average optical powers and number of bases.

B. *Noise Masking by ASE-Signal Beat Noise*

Additive noises, such as ASE noise, also provides noise masking. Therefore, it is essential to discuss the noise masking phenomenon achieved by ASE-signal beat noise. Here, the ASE-ASE beat noise is ignored because it is negligibly small compared to the ASE-signal beat noise in our cipher system. The standard deviation of the noise is represented by

$$\sigma_{ASE} = \sqrt{\frac{2BP_0^2}{R_{REF}OSNR}}, \qquad (5)$$

where $\mathrm{R_{REF}}$ is the bandwidth of reference, typically, 12 GHz (0.1 nm), and OSNR denotes the optical signal-to-noise ratio (OSNR) of the IM Y-00 cipher signal. The amount of noise masking is derived by

$$\Gamma_{IM} = \frac{2\sigma_{ASE}}{\Delta P_{basis}} = \frac{2(2M-1)P_0}{(P_{2M}-P_1)}\sqrt{\frac{2B}{R_{REF}OSNR}} \qquad (6)$$

Similar to the case of noise masking by shot noise, the DC offset of $\mathrm{P_1}$ ($\neq 0$) prevents the condition of no noise masking on the lowest power level of Y-00 cipher signals. Noise masking is dependent on a signal power. The amount of noise masking of $\mathrm{P_{2M}}$ is *r* times higher than that of $\mathrm{P_1}$. By substituting the ratio of maximum power to minimum power $\mathrm{r} = \mathrm{P_{2M}} / \mathrm{P_1}$ and $\mathrm{P_0} = \mathrm{P_M}$ ($= (\mathrm{P_{2M}} + \mathrm{P_1}) / 2$) in (6), we obtain

$$\Gamma_{IM} = \frac{(2M-1)(r+1)}{r-1}\sqrt{\frac{2B}{R_{REF}}\cdot\frac{1}{OSNR}} \qquad (7)$$

Γ_{IM} has a smaller value for a higher OSNR. Noise masking is numerically calculated using (7) for the bases numbers of $\mathrm{M} = 2^9, 2^{10}, 2^{11}$, and 2^{12}, when OSNR is changed. The noise masking number of 200 is achieved for $\mathrm{M} = 2^{11}$, when $\mathrm{OSNR} = 30$ dB as shown in Fig. 8. Even with a lower basis number of $\mathrm{M} = 2^9$, a noise masking number of 150 is achievable for $\mathrm{OSNR} = 20$ dB.

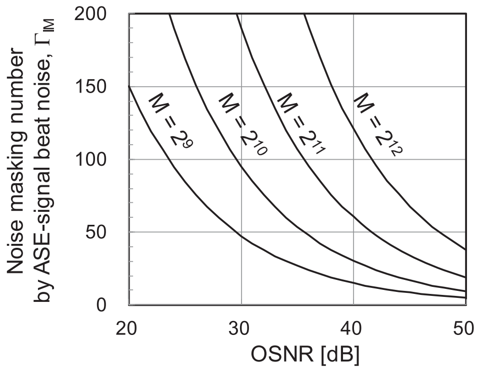


Fig. 8. Noise masking number by ASE-signal beat noise of the IM Y-00 cipher as a function of OSNR (optical signal-to-noise ratio) and the number of bases.

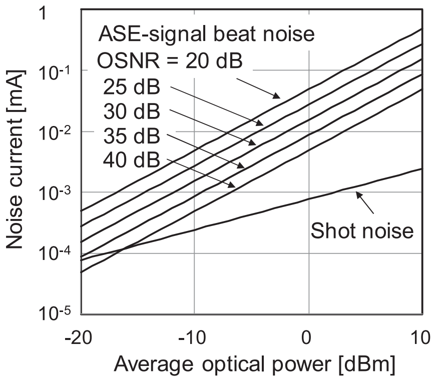


Fig. 9. Noise amount of shot noise and ASE-signal beat noise.

C. Comparison of the Amounts of Shot Noise and Beat Noise

The amounts of shot noise and ASE-signal beat noise are compared. Fig. 9 summarizes the noise amounts with respect to the typical parameters in a practical Y-00 cipher communication system. It is observed from this figure that the ASE-signal beat noise is higher than the shot noise for the higher signal powers. The difference is smaller for the lower signal powers, and the shot noise is higher than the ASE-signal beat noise, for instance, for the signal power of -20 dBm and the OSNR of 40 dB.

IV. Probability of Guessing the Ciphertext Accurately

To date, Y-00 cipher security has been theoretically investigated, and the general property of the Y-00 cipher has been clarified [28]. In our previous work, the probability of an attacker failing to guess the ciphertext accurately was discussed [21]. In this section, the probability of an attacker guessing the correct ciphertext is discussed under some assumptions [34]. It is assumed that an attacker observes the Y-00 cipher, i.e., multi-level signals with the same power difference, and tries estimating the correct power level. It is also assumed that direct detection is performed, and the probability distributions of the measurement result are shown in Fig. 10 is approximated by Gaussian. Furthermore, to simplify our analysis, we assumed that each standard deviation of the distribution is represented by the average value when P_0

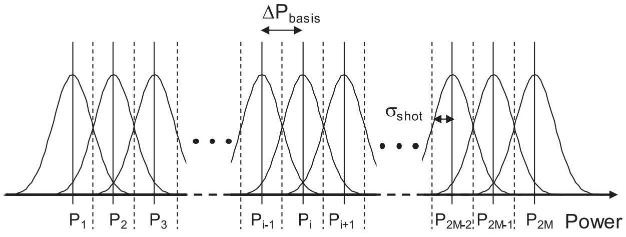


Fig. 10. Model of measurement results by an attacker for multi-level IM signals.

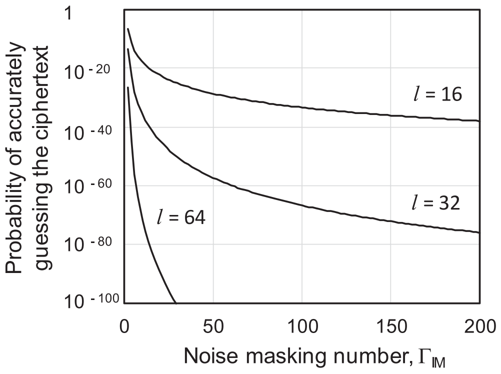


Fig. 11. Probability of guessing the ciphertext accurately.

$= \mathrm{P}_{\mathrm{M}}$, although it is not strictly the same as mentioned in the previous section. The probability of correct signal detection at a single time slot is derived under these assumptions as

$$P_{single} = 1 - \frac{2M-1}{2M} erfc\left[\frac{1}{\sqrt{2\Gamma}}\right], \tag{8}$$

where erfc[$\cdot$] is the complementary error function and Γ denotes Γ_{IM_shot} or Γ_{IM}. The probability of correct signal detection at a single time slot is expressed by the parameters, such as the number of bases and the amount of noise masking. Considering that the number of bases is high, (8) is approximately expressed using only Γ as

$$P_{single} \approx erf\left[\frac{1}{\sqrt{2\Gamma}}\right], \tag{9}$$

where erf[$\cdot$] is the error function. The probability at a single time slot has been discussed so far. However, the signal detections of successive time slots are required for intercepting the data or key. The probability in such cases is expressed using the successive number l as

$$P_{key} = (P_{single})^l \tag{10}$$

The successive number l is related to the key length and mathematical complexity, which is beyond the scope of this work. Fig. 11 shows the probability of correctly guessing the successive time slots. A higher masking number and a longer l are necessary for ensuring a better security of the system. The probability can be easily decreased by employing a higher number of bases. It should be noted that the entire secrecy of Y-00 cipher is not evaluated only by the probability. The complexity of

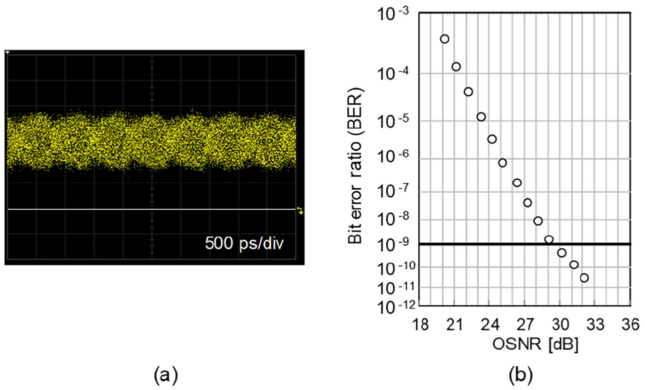


Fig. 12. 1.5-Gb/s IM Y-00 cipher with 4096 intensity levels. (a) An eye-diagram measured by a photodetector with DC couple, and (b) the bit error ratio.

mathematical randomization, namely the generation scheme of the pseudo-random number, must also be considered. However, the above analysis is effective in estimating the secrecy of the Y-00 cipher communication system.

V. Security Assessment of the Transmission System

We demonstrate real-time 1,000-km cipher transmission at 1.5 Gb/s using a Y-00 cipher transceiver we developed [25]. In this section, the noise masking phenomenon is experimentally measured, and the probabilities of accurately guessing the ciphertext in the transmission system are evaluated.

A. 1,000-km Transmission Using a Y-00 Cipher Transceiver

In the transmitter of a Y-00 cipher transceiver [19], a binary signal is modulated at 1.5 Gb/s using a $LiNbO_3$ Mach-Zehnder modulator, for which the bias is set on a bit-by-bit basis based on a stream of pseudo-random numbers (PRNs), as mentioned in section II. In the transceiver, a linear feedback shift register (LFSR) is employed as a simple PRNG. The PRNs are generated by extending the initial key of 256 bits to a key of length 2^{256} - 1 with the LFSR. The 256-bit initial key is a pre-shared secret between the transmitter and receiver. The number of bias levels M is set to 2048 (=2^{11}), and consequently, Y-00 optical cipher signals with 4096 intensity levels are generated using a DAC with a 12-bit nominal resolution. The effective resolution might be smaller, which, in practice, will result in an enhancement of the noise masking effect, provided that the noise is considered to be random. The power ratio r of the highest cipher signal to the lowest (P_{2M} / P_1) is set to 2.0 by adding a DC voltage to a Mach–Zehnder modulator (Fig. 12(a)). The binary data is a pseudo-random bit sequence (PRBS) with a length of 2^{31} - 1. The wavelength of the Y-00 cipher signal is set to 1550.12 nm. In the receiver of the Y-00 cipher transceiver, the incoming Y-00 cipher signal is converted to an electrical signal by direct detection with AC coupling. Then the multi-level electrical signal is then decrypted to a binary signal by changing the threshold level of the binary signal decision circuit in a bit-by-bit manner using the same PRNs generated from the key shared between the transmitter and receiver. The bit error ratio (BER) values obtained are shown in Fig. 12(b). The OSNR is set by adding ASE noise from an optical amplifier to the signal, and an optical bandpass filter (OBPF) with a 3-dB bandwidth of 0.5 nm was used to suppress out-of-band ASE noise. The OSNR required for achieving BER of 10^{-9} is 30 dB, which is higher than that required for on–off keying. This is the drawback of the high security in the intensity-modulated Y-00 cipher. The required OSNR is smaller if the power ratio, r, is set to a lower value, although the level of security is reduced. The relationship between the power ratio and the probability that an attacker will detect the wrong intensity level is described in [21]. An eye-diagram of the Y-00 signal measured with a photodetector of 12.4 GHz with DC coupling is shown in Fig. 12(a). The white horizontal line indicates the absence of optical power as a reference line. The eye looks closed, as the power difference between the neighboring power levels is as low as 1 μW, when the average power of the Y-00 signal is 6 dBm.

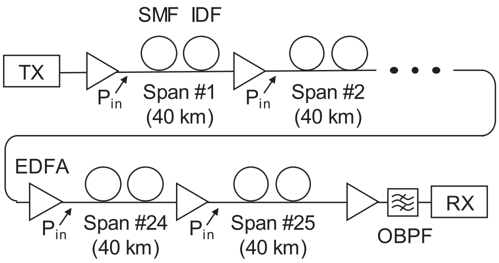


Fig. 13. Experimental setup for the 1,000-km transmission of 1.5-Gb/s IM Y-00 cipher (SMF - single mode fiber, IDF - inverse dispersion fiber, EDFA-erbium-doped fiber amplifier, TX and RX - transmitter and receiver of the Y-00 cipher transceiver, respectively).

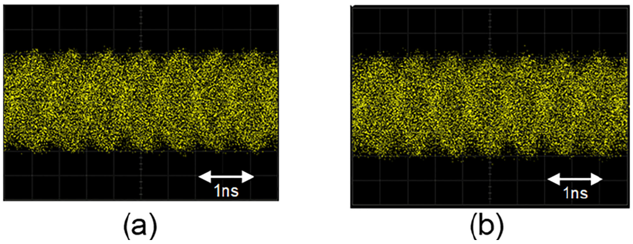


Fig. 14. Eye diagrams of the IM Y-00 cipher of 4096 intensity levels measured using a photodetector with AC coupling at (a) 0 km and (b) 1,000 km.

Fig. 13 shows the setup of our transmission experiment. The setup comprises the transmitter (TX) and receiver (RX) of the Y-00 cipher transceiver and the dispersion-managed link. The span of the link comprises a single mode fiber (SMF) with a large effective area and an inverse dispersion fiber (IDF). The length and the average loss of each span are 40 km and 11.1 dB, respectively. The transmission link included 25 spans and 25 optical amplifiers (erbium-doped fiber amplifiers (EDFAs)), and the total length is 1,000 km. The optical powers launched on all spans (P_{in}) are set to be similar. The eye-diagrams are measured using a photodetector of 12.4-GHz bandwidth with AC coupling. Both the eye-diagrams at 0 km and 1,000 km (Figs. 14(a) and 13(b)) appear noisy, as the noise masks the adjacent levels of

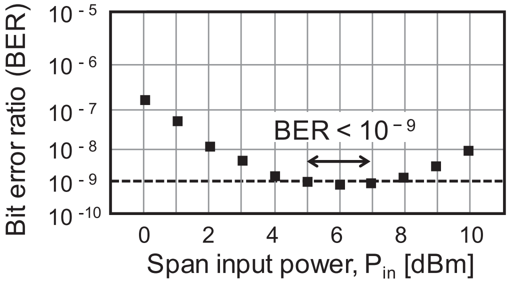


Fig. 15. Bit error ratio (BER) at 1,000 km for span input powers.

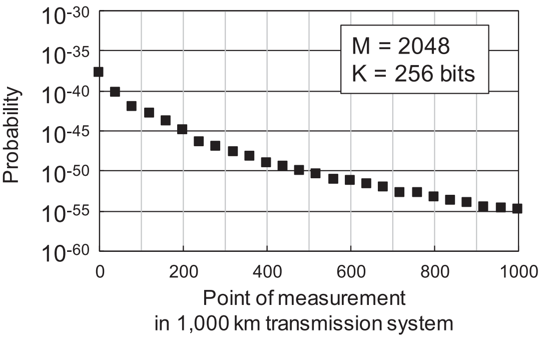


Fig. 16. Probability of accurately guessing the ciphertext.

signals. The BER of the binary data (PRBS: 2^{31}-1) is measured after Y-00 decryption. Fig. 15 summarizes the BERs for input powers with respect to each span ($\mathrm{P_{in}} = 0$ –10 dBm). For input powers from 5 – 7 dBm, an error-free transmission with BER $< 10^{-9}$ is demonstrated. When $\mathrm{P_{in}}$ is further increased, the BER values decrease due to the nonlinear effect caused in optical fibers of the dispersion-managed link. When $\mathrm{P_{in}}$ is decreased, the OSNR values also decrease, thereby resulting in very low BER values.

B. Security Assessment

The probabilities of guessing the ciphertext accurately are evaluated in the 1,000-km transmission link using the analytical solution derived in the previous section, when $\mathrm{P_{in}}$ is set to 6 dBm for achieving a BER of $< 10^{-9}$ after the 1,000-km transmission. The maximum noise masking number of the shot noise in the transmission link is calculated using (3) to be $\Gamma_{\mathrm{IM\_shot}} = 19.5$ when the shot noise is calculated to be 0.45 μA using (1). The shot noise covers more than 19 levels of different Y-00 signal intensities. The noise masking number of the ASE-signal beat noise is measured in the following way. First, the OSNR value is experimentally measured and then the noise masking number, Γ_{IM}, is calculated using (7). The ASE noise and shot noise are included in the masking effect since the noise of the measured OSNR also contains shot noise. The OSNR values of the Y-00 cipher signals from each EDFA are measured. The minimum value is $\Gamma_{\mathrm{IM}} = 33.8$ at the output from the transmitter and increases along the transmission link. The maximum value is $\Gamma_{\mathrm{IM}} = 190$ after the last EDFA. Next, the probabilities of guessing the ciphertext accurately are calculated using measured Γ_{IM} and (10). In the calculation, l is set to 23, as the LFSR is utilized in the transceiver as a PRNG [34]. The probabilities are plotted in Fig. 16 as a function of a measurement point in the 1,000-km transmission system. The minimum probability of 1.7×10^{-55} ($\Gamma_{\mathrm{IM}} = 190$) is observed at the receiver end, for which the OSNR is a minimum, whereas the maximum probability of 1.6×10^{-38} ($\Gamma_{\mathrm{IM}} = 33.8$) is observed at the transmitter end, for which the OSNR is a maximum. Thus, it is established that even when an LFSR is utilized as a simple PRNG, the probability of the transmission system is lower than 10^{-37}. Therefore, we can easily decrease the probability either by setting a higher number of signals levels and/or by employing more complicated PRNG.

VI. Conclusion

We presented the basic concept, noise masking phenomenon, and the operation principle of the Y-00 cipher for data encryption. The noise masking required for restricting the interception of ciphertext by the attackers was generated by the shot noise, i.e., quantum noise and ASE-signal beat noise. The noise masking parameters of both noise were derived and compared for the Y-00 cipher with intensity modulation. In addition, an approximate analytical solution of the intensity modulated Y-00 cipher to evaluate the probability of accurately guessing the cipher text was discussed. The solution was applied to evaluate the secrecy of the intensity modulated Y-00 cipher transmission system of 1,000 km with inline optical amplifiers at a bit rate of 1.5 Gb/s. In the transmission system using optical repeater amplifiers, careful design of the system parameters such as the basis number, M, power ratio, r, data rate, B, and OSNR is required to achieve the target security level of the transmission system.

Acknowledgment

The authors would like to thank O. Hirota for his support for this work.

References

[1] C. H. Bennett, and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984, pp. 175–179.

[2] V. Annovazzi-Lodi, S. Donati, and A. Scire, “Synchronization of chaotic injected-laser systems and its application to optical cryptography,” *IEEE J. Quantum Electron.*, vol. 32, no. 6, pp. 953–959, Jun. 1996.

[3] T. H. Shake, “Security performance of optical CDMA against eavesdropping,” *IEEE J. Lightw. Technol.*, vol. 23, no. 2, pp. 665–670, Feb. 2005.

[4] H. P. Yuen, “KCQ: A new approach to quantum cryptography I. General principles and key generation,” Nov. 2003. [Online]. Available: https://arXiv:quant-ph/0311061v6

[5] F. Futami, K. Tanizawa, and K. Kato, “Y-00 quantum stream cipher for physical layer security of optical communications,” in *Proc. Eur. Conf. Opt. Commun.*, Dublin, Ireland, Sep. 2019, Paper Th.2.E.1.

[6] G. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure communication using mesoscopic coherent states,” *Phys. Rev. Lett.*, vol. 90, no. 22, Jun. 2003, Art. no. 227901.

[7] 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, no. 6, Jun. 2005, Art. no. 062326.

[8] 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, no. 2, Aug. 2005, Art. no. 022335.

[9] K. Kato, and O. Hirota, "Quantum quadrature amplitude modulation system and its applicability to coherent state quantum cryptography," *Proc. SPIE*, vol. 5893, 2005, Art. no. 589303.

[10] G. S. Kanter, D. Reilly, and N. Smith, "Practical physical-layer encryption: the marriage of optical noise with traditional cryptography," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 74–81, Nov. 2009.

[11] Y. Doi, S. Akutsu, M. Honda, K. Harasawa, O. Hirota, S. Kawanishi, O. Kenichi, and K. Yamashitaet, "360 km field transmission of 10 Gbit/s stream cipher by quantum noise for optical network," in *Proc. Opt. Fiber Comm. Conf.*, San Diego, CA, USA, 2010, Paper OWC4.

[12] K. Ohhata, O. Hirota, M. Honda, S. Akutsu, Y. Doi, K. Harasawa, and K. Yamashita, "10-Gb/s optical transceiver using the Yuen 2000 encryption protocol," *IEEE J. Lightw. Technol.*, vol. 28, no. 18, pp. 2714–2723, Sep. 2010.

[13] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, T. Hosoi, and Y. Doi, "Quantum encryption communication over a 192-km 2.5-Gbit/s line with optical transceivers employing Yuen-2000 protocol based on intensity modulation," *IEEE J. Lightw. Technol.*, vol. 29, no. 3, pp. 361–323, Feb. 2011.

[14] F. Futami, and O. Hirota, "Transmission of Y-00 quantum cipher from transmitter using directly modulated DFB laser for secure access networks," in *Proc. Int. Conf. Photon. Switching*, Ajaccio, France, 2012, Paper Th-S14-O08.

[15] M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai, "QAM quantum stream cipher using digital coherent optical transmission," *Opt. Express*, vol. 22, no. 4, pp. 4098–4107, Feb. 2014.

[16] F. Futami and O. Hirota, "100 Gbit/s (10 × 10 Gbit/s) Y-00 cipher transmission over 120 km for secure optical fiber communication between data centers," in *Proc. OECC/ACOFT2014*, Melbourne, Australia, 2014, Paper MO1A2.

[17] F. Futami, and O. Hirota, "Demonstration of 2.5 Gbit/sec free space optical communication by using Y-00 cipher: toward secure aviation systems," *Proc. SPIE,* vol. 9202, 2014, Art. no. 92020R.

[18] F. Futami, "Experimental demonstrations of Y-00 cipher for high capacity and secure optical fiber communications," *Quantum Inform. Process.*, vol. 13, no. 10, pp. 2277–2291, Oct. 2014.

[19] F. Futami, K. Kato, and O. Hirota, "A novel transceiver of the Y-00 quantum stream cipher with the randomization technique for optical communication with higher security performance," *Proc. SPIE*, vol. 9980, 2016, Art. no. 99800O.

[20] M. Nakazawa *et al.*, "QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution," *IEEE J. Quantum Electron.*, vol. 53, no. 4, Aug. 2017, Art. no. 8000316.

[21] F. Futami *et al.*, "Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system," *Opt. Express*, vol. 25, no. 26, pp. 33338–33349, Dec. 2017.

[22] F. Futami, T. Kurosu, K. Tanizawa, K. Kato, S. Suda, and S. Namiki, "Dynamic routing of Y-00 quantum stream cipher in field-deployed dynamic optical path network," in *Proc. Opt. Fiber Comm. Conf.*, San Diego, CA, USA, 2018, Paper Tu2G.5.

[23] K. Tanizawa and F. Futami, "2^{14} intensity-level 10-Gbaud Y-00 quantum stream cipher enabled by coarse-to-fine modulation," *IEEE Photon. Tech. Lett.*, vol. 30, no. 22, pp. 1987–1990, Nov. 2018.

[24] K. Tanizawa and F. Futami, "Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels," *Opt. Express* vol. 27, no. 2, pp. 1071–1079, Jan. 2019.

[25] F. Futami, K. Tanizawa, K. Kato, and O. Hirota, "1,000-km transmission of 1.5-Gb/s Y-00 quantum stream cipher using 4096-level intensity modulation signals," in *Proc. Conf. Lasers Electro-Opt.*, San Jose, CA, USA, 2019, Paper SW3O.4.

[26] 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, no. 18, pp. 25357–25363, Sep. 2019.

[27] F. Futami, and O. Hirota, "Masking of 4096-level intensity modulation signals by noises for secure communication employing Y-00 cipher protocol," in *Proc. Eur. Conf. Opt. Commun.*, Geneva, Switzerland, 2011, Paper Tu.6.C.4.

[28] O. Hirota, "Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol," *Phys. Rev. A*, vol. 76, no. 3, Sep. 2007, Art. no. 032307.

[29] T. Shimizu, O. Hirota, and Y. Nagasako, "Running key mapping in quantum stream cipher by Yuen 2000 protocol," *Phys. Rev. A*, vol. 77, Mar. 2008, Art. no. 034305.

[30] K. Kato, and O. Hirota, "Randomization techniques for the intensity modulation-based quantum stream cipher and progress of experiment," *Proc. SPIE*, vol. 8168, 2011, Art. no. 81630A.

[31] K. Kato, "Quantum enigma cipher as a generalization of the quantum stream cipher," *Proc. SPIE*, vol. 9980, 2016, Art. no. 998005.

[32] K. Kato, "A unified analysis of optical signal modulation formats for quantum enigma cipher," *Proc. SPIE*, vol. 10409, 2017, Art. no. 104090K.

[33] F. Futami, K. Tanizawa, K. Kato, and O. Hirota, "Experimental investigation of security parameters of Y-00 quantum stream cipher transceiver with randomization technique: Part I," *Proc. SPIE*, vol. 10409, 2017, Art. no. 104090I.

[34] F. Futami, K. Tanizawa, K. Kato, and O. Hirota, "Experimental investigation of security parameters of Y-00 quantum stream cipher transceiver with randomization technique: Part II," *Proc. SPIE*, vol. 10771, 2018, Art. no. 1077114.

Fumio Futami (Member, IEEE) received the B.S., M.S., and Ph.D. degrees all in electronic engineering from the University of Tokyo, Tokyo, Japan, in 1995, 1997, and 2000, respectively. In 2000, he joined Fujitsu Laboratories Ltd., Kawasaki, Japan, where he was mainly engaged in the research and development of ultra-high speed optical transmission systems and ultra-fast all-optical signal processing for optical communication systems. In 2010, he moved to Tamagawa University, Tokyo, and began the research and development of the cipher communication employing physical phenomena for achieving high secrecy and high communication performance. He was promoted to a Professor in 2014 and has been serving as a Steering Committee Member of CLEO PR since 2016, and as a Technical Program Committee Member of OFC since 2019. He is a member of OSA, SPIE, and IEICE.

Ken Tanizawa (Member, IEEE) received the B.E., M.E., and Ph.D. degrees all in electronic engineering from the University of Tokyo, Tokyo, Japan, in 2004, 2006, and 2009, respectively. From 2007 to 2009, he was a Research Fellow with the Japan Society for the Promotion of Science. From 2009 to 2017, he was with the National Institute of Advanced Industrial Science and Technology (AIST), Japan, where he was involved in the researche on silicon photonics and optical signal processing. In 2017, he joined Tamagawa University where he is currently an Associate Professor with Quantum ICT Research Institute. His research interests include secure optical transmission systems and silicon photonics devices for communications and computing. He is a member of the Institute of Electronics, Information, and Communication Engineers of Japan.

Kentaro Kato (Member, IEEE) received the Ph.D. degree in information and communications engineering from Tamagawa University, Tokyo, Japan, in 2001. Since 2011, he has been with Tamagawa University, where he is currently a Professor with Quantum Information Science Research Center, Quantum ICT Research Institute of Tamagawa. His research interests include quantum signal detection theory, quantum information theory, quantum communications, quantum cryptography, and quantum sensing. He is a member of OSA, SPIE, and APS.