PHOTONICS Research

High-speed optical secure communication with external noise source and internal time-delayed feedback loop

Yudi Fu, Mengfan Cheng,* Xingxing Jiang, Quan Yu, Linbojie Huang, Lei Deng, and Deming Liu

National Engineering Laboratory for Next Generation Internet Access System (NGIA), School of Optical and Electronic Information, Huazhong University of Science and Technology (HUST), Wuhan 430074, China

**Corresponding author: Chengmf@mail.hust.edu.cn*

Received 3 July 2019; revised 7 September 2019; accepted 10 September 2019; posted 11 September 2019 (Doc. ID 371592); published 31 October 2019

We propose and experimentally demonstrate a novel physical layer encryption scheme for high-speed optical communication. A 10 Gb/s on-off keying signal is secretly transmitted over 100 km standard single-mode fiber. The intensity-modulated message is secured by the encryption mechanism, which is composed of an external noise source and an internal time-delayed feedback loop. The external noise serves as an entropy source with sufficient randomness. The feedback loop structure in the transmitter introduces a time-domain encryption key space, and a corresponding open-loop configuration at the receiver side is used for synchronization and decryption. Experiment results show the effectiveness of the proposed scheme. For a legitimate terminal, bit error rate below 10^{-8} can be obtained. Decryption degradations with the mismatch of different hardware parameters are researched. The time delay in the feedback loop provides a sensitive encryption key. For other hardware parameters, the system is robust enough for synchronization. Meanwhile, the time-delay signature of the loop is able to be well concealed by the external noise. Moreover, the proposed scheme can support density wavelength division multiplexing transmission with a relatively simple structure. This work also provides a new concept to establish optical secure communication by combining a time-delayed feedback chaotic system and random noise.

https://doi.org/10.1364/PRJ.7.001306

1. INTRODUCTION

With the explosive growth of data information and knowledge, optical-fiber communication is developing towards high-speed, broadband, and large-capacity communication networks. It will be difficult to meet the requirements of high-capacity data transmission and information security simultaneously. The security performance of traditional strategies such as cryptography and authentication protocols at the media access control layer or higher layers is potentially limited by the processing speed of electronics and the capacity of optical networks [1,2]. In the past decade, secure optical communication with a physical layer protection technique such as optical encryption and steganography has been developed [3–6]. These optical domain strategies can support high throughput and further enhance the security of communication systems.

Conceptually, encryption at the physical layer is to bury a plain-text signal into a random or pseudo-random signal in various ways. Therefore, an entropy source with sufficient randomness or complexity is indispensable. As a typical noise source in an optical field, amplified spontaneous emission (ASE) noise has been used as an ultrawideband entropy source in secure communications [7–9]. In these schemes, noise embedded with data and a pure noise signal are transmitted through the fiber link with a time difference. At the receiver side, only when the time delay is accurately fixed can the data signal be extracted by canceling the noise. The data signal is well hidden within the noise in both time and frequency domains. The broadband nature of ASE noise makes the time delay a very sensitive encryption key. An optical delay line (DL) with highly adjustable precision enables a legal receiver to match the key precisely. As a result, a time domain large key space can be established [10]. However, the interference mechanism degrades the optical signal-to-noise ratio (OSNR) and suppresses the maximum data transfer rate of a single wavelength to 1 Gb/s [11]. Besides, beating the modulated ASE and the reference ASE from different light paths might impact the stability of data decryption. Thus, the decryption can be held in just several seconds because of the sensitive interference structure [7]. Meanwhile, the time delay could be extracted by an unauthorized third party using some statistical methods, such as cross-correlation function or delayed mutual information.

This issue has attracted some attention recently because it may cause a potential security risk [12].

Optical chaos is another entropy source that has been widely investigated in secure communication systems [13–17]. Using broadband chaos as the optical carrier, secure communication at a data rate of 30 Gb/s over 100 km fiber link has been reported [18]. Due to the inner feedback structure, only the data-buried chaotic signal is needed to transmit in the link, while the pure chaotic carrier can be recovered at the receiver using a synchronization mechanism. Thus, high-speed transmission can be achieved. The security of chaos-based systems also relies on the large key space depending on high-precision physical parameters, especially the delay time [19,20]. However, a time delay signature (TDS) may significantly affect the security level of chaos communication systems [21,22], and eavesdroppers could reconstruct the phase space with TDS. Consequently, the communication system is exposed to danger. To solve this problem, much research has been reported [23–37]. Among them, Jiang *et al.* suggested several ways to successfully conceal the TDS, such as modified feedback approaches [25], digital phase mask [29], and optical time lens [36]. Li *et al.* proposed the scheme of optical injection [31]. Xia *et al.* reported a TDS method with system coupling [35]. In addition, bandwidth and complexity enhancement are also critical issues in chaotic systems [25,31,38–40]. When these facts are considered simultaneously, the implementation complexity of a chaotic system could be increased markedly. Chaos synchronization may also become a challenge under these preconditions.

By comparing these two types of optical encryption methods, we can find that the chaos system has the advantage in ready synchronization and high-speed data extraction, especially for those systems with internal electro-optical feedback structures [3,13,18]. For the strategies with an external noise source, there are also notable advantages. First, the bandwidth of the noise signal such as the ASE noise could be very large. From the viewpoint of an independent entropy source, it is speculated that the randomness or complexity of a truly random noise signal is higher than that of the chaotic one [41].

In this paper, we propose a novel physical layer encryption scheme with both the external random noise source and internal feedback loop structure. Secure data transmission over 100 km standard single-mode fiber (SSMF) with the rate of 10 Gb/s is experimentally demonstrated. The sensitivity of secret keys is quantitatively analyzed to ensure system security, according to our previous work [42]. TDS concealment and complexity performance are quantitatively investigated. Last but not least, a density wavelength division multiplexing (DWDM) scheme with the channel spacing of 50 GHz is experimentally demonstrated without performance regressions, which shows its potential in supporting high-capacity long-haul secure communications.

2. PRINCIPLE AND EXPERIMENTAL SETUP

The schematic diagram of the proposed system is shown in Fig. 1. Before the encryptor, a normal intensity-modulated (IM) signal acts as the data source. The optical data signal is then injected into the optical domain encryptor, which is composed of a phase noise module and a self-phase-modulated feedback (SPMF) module. In the first module, the data are masked in both phase and intensity field by the dispersion-induced phase modulation to intensity modulation (PM-to-IM) conversion [43]. Here we use a tunable fiber Bragg grating (FBG1) (TDCMB-C000-NC-BF01) as the dispersion medium. Then the SPMF module is used to further distort the phase, and a controllable time delay is introduced in the feedback loop to create a large key space. The encrypted signal is then transmitted over the fiber link. At the receiver side, a symmetrical SPMF module is used to decrypt the phase. The original IM data are detected after FBG4 (TDCMB-C000-NC-BF01), which reverses the PM-to-IM conversion process.

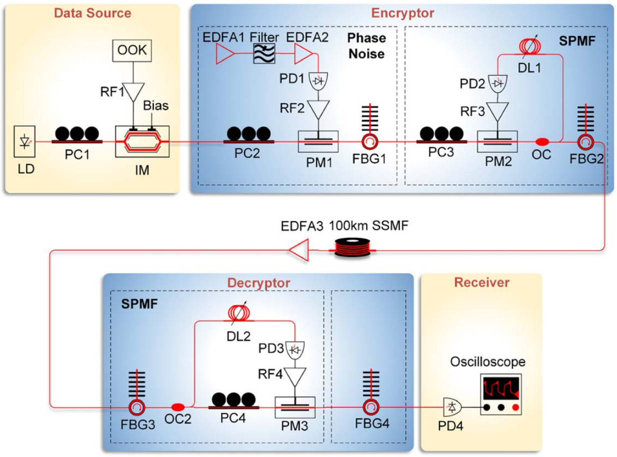

Fig. 1. Experimental setup of the secure communication system. LD, tunable laser diode; PC, polarization controller; RF, radio-frequency amplifier; IM, intensity modulator; EDFA, erbium-doped fiber amplifier; PD, photodetector; PM, phase modulator; FBG, fiber Bragg grating; DL, tunable delay line; OC, optical coupler; SSMF, standard single-mode fiber; SPMF, self-phase-modulated optical feedback.

A laser diode (LD) (TLG-200) with central wavelength of 1551.19 nm and optical power of 13.5 dBm is adopted to provide the optical carrier. An amplified 10 Gb/s non-return-to-zero on-off keying (NRZ-OOK) data $m(t)$ is used to drive an intensity modulator that is working in its linear zone. The electrical field of the intensity-modulated signal $E_0(t)$ could be expressed by the equation

$$E_0(t) = \sqrt{P_0} m(t) \exp(j\omega_0 t + \Phi_0), \tag{1}$$

where ω_0 is the angular frequency and $\Phi_0 = \pi/2$. P_0 is the optical power.

$E_0(t)$ is then distorted in phase through a phase modulator (PM1) (PM-DS5-20-PFA-PFA-LV). The ASE noise from an erbium-doped fiber amplifier (EDFA1) is used as the entropy source after being filtered by an optical filter and amplified by EDFA2. The frequency responses of the photodetector (PD1) and radio-frequency amplifier (RF2) also limit the bandwidth of the noise to 10 GHz. Then the broadband noise is input to the electrode of PM1 whose RF half-wave voltage is 3.9 V. The output light of PM1 can be written as

$$E_p(t) = E_0(t) \exp[j\pi C_1 n(t)^2], \tag{2}$$

where $n(t)$ is the normalized noise signal and $C_1 = 0.64$ is the modulation depth. The peak-to-peak value of the output voltage of PD1 is measured as 320 mV, and the gain of RF2 is 18 dB.

The transfer function of the dispersion in frequency domain can be described as

$$H(\omega) = \exp\left[j\frac{B}{2}(\omega - \omega_0)^2\right], \tag{3}$$

where B is the accumulated second-order dispersion. The output lightwave of FBG1 is

$$E_p'(t) = F^{-1}\{F[E_p(t)]H(\omega)\}, \tag{4}$$

where $F(\cdot)$ denotes the Fourier transform.

Reflected from FBG1, $E_p'(t)$ is sent into the SPMF module. The signal is modulated by PM2 (PM-DS5-20-PFA-PFA-LV), whose RF half-wave voltage is 3.9 V. After an optical coupler (OC1) and a tunable optical fiber DL1, the optical signal is detected by PD2. Before being fed back into the electrode of PM1, the generated electrical signal is amplified by RF3. Another output beam from OC1 is sent into 100 km SSMF after FBG2 (TDCMB-C000-NC-BF01). The mathematical model of the SPMF loop can be derived as

$$V(t) + \tau\frac{\mathrm{d}V(t)}{\mathrm{d}t} + \frac{1}{\theta}\int_{t_n}^{t} V(\varepsilon)\mathrm{d}\varepsilon = \eta GS|E_p'(t - t_D)|^2, \tag{5}$$

where $V(t)$ is the drive voltage of PM2, and τ and θ are the characteristic response times of the bandpass filter, which is composed of RF3 and PD2. The bandwidth of PD2 is 10 GHz. t_D is the delay time of the whole loop. η is the optical attenuation factor; G is the gain of RF3; S is the sensitivity of PD2. The modulation depth of PM2 $\beta = \eta GS$ is calculated to be 0.4.

At the receiver side, a symmetrical setup is designed for decryption. FBG3 (TDCMB-C000-NC-BF01) is used to compensate the overall dispersion of FBG2 and the transmission link. In the SPMF module of the decryptor, an inverse PD (PD3) with the bandwidth of 10 GHz, which is established with a differential output photodiode in our experiment, is adopted to generate a voltage opposite that of PD2. Therefore, the scrambled phase in PM2 can be canceled after PM3 (PM-DS5-20-PFA-PFA). The original IM signal can be detected by PD4 after FBG4, whose dispersion coefficient is opposite that of FBG1.

In the setup, the signal is encrypted with a three-dimensional key: the dispersion coefficients of FBG1 and FBG2, and the delay time of the SPMF. Meanwhile, the optical domain encryptor and decryptor can be directly inserted into the optical link without any modification to the original intensity modulation direct detection (IM/DD) system. This fact means that the proposed scheme has a good compatibility with existing facilities.

3. MAIN RESULTS

A digital serial analyzer (DSA 72504D) with a sampling rate of 100 GSample/s is used to record the time traces of the system output under different circumstances. The cumulative dispersions of FBG1 and FBG2 are set as −800 ps/nm and −1200 ps/nm, respectively. Accordingly, the cumulative dispersions of FBG3 and FBG4 are set as −500 ps/nm and 800 ps/nm.

As a contrast, we demonstrate the performance of the transmission link without using any encryption strategy. A common 10 Gb/s NRZ-OOK signal is intensity-modulated and transmitted over 100 km SSMF. Figures 2(a) and 2(d) show the waveform and the corresponding eye diagram. Then we enable the encryption strategy. After the encrytor, the IM signal is significantly distorted, as shown in Figs. 2(b) and 2(e). Since the physical parameters such as the dispersion, the delay time, and the modulation coefficient in the encryptor and decryptor are well matched, the data recovery can be effectively achieved at the receiver side, as shown in Figs. 2(c) and 2(f). Note that the sequences are plotted in Fig. 2(a).

Similar conclusions can be obtained from spectrum analysis. Figure 3(a) presents the RF spectrum of the IM data signal. After the encryptor, the spectrum is flattened, as shown in Fig. 3(b), which indicates the data are buried in the noise. Correspondingly, the spectrum of the well-decrypted signal is shown in Fig. 3(c).

Note that the sequences plotted in Figs. 2(a) and 2(c) do not correspond in time because after long-haul transmission, it is difficult to save the original data sequence and the corresponding recovered sequence simultaneously. The curves in Fig. 2 only indicate the general performance of encryption and decryption. The bit error rate (BER) performance under the aforementioned circumstances is measured by a bit error tester (BERTWave E410A), which provides a pseudo random binary sequence (PRBS) with the length of $2^{31} - 1$ and receives the feedback recovered sequence to present a BER value. A BER below 10^{-8} is measured for the legitimate individual after good decryption. On the contrary, the BER of an intruder in the fiber link (the test point is at the output of EDFA3) exceeds the measurement range of the BER tester. When the BER of

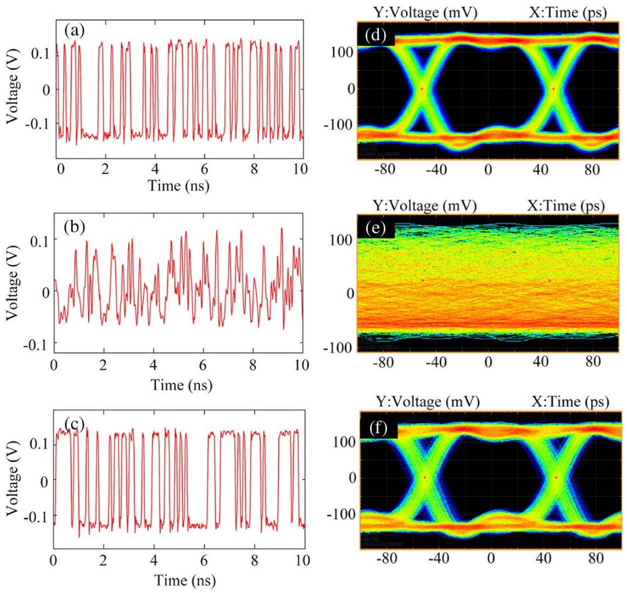

Fig. 2. (a) Time series of the original data signal at the output of intensity modulator; (b) time series of the encrypted signal at the output of FBG2; (c) time series of the decrypted signal at the output of FBG4; (d) eye diagram of the original data signal at the output of intensity modulator; (e) eye diagram of the encrypted signal at the output of FBG2; (f) eye diagram of the decrypted signal at the output of FBG4.

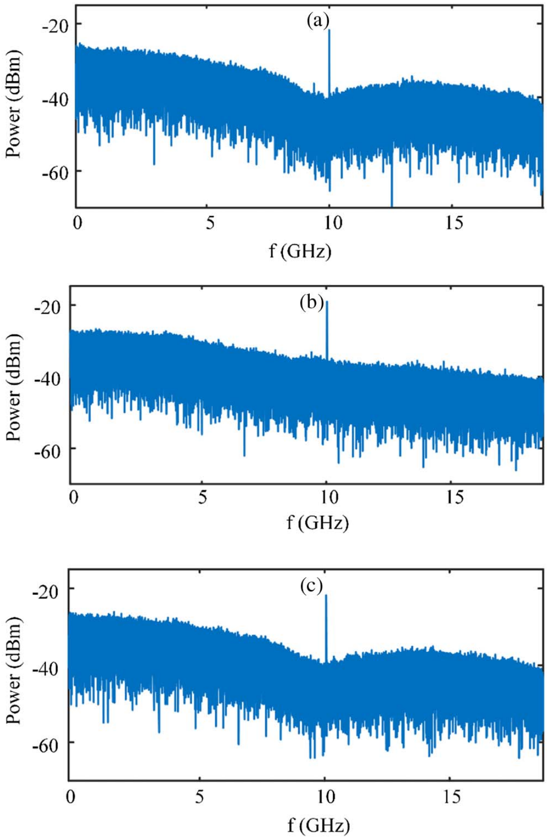

Fig. 3. (a) RF spectrum of the data signal; (b) RF spectrum of the encrypted signal; (c) RF spectrum of the decrypted signal.

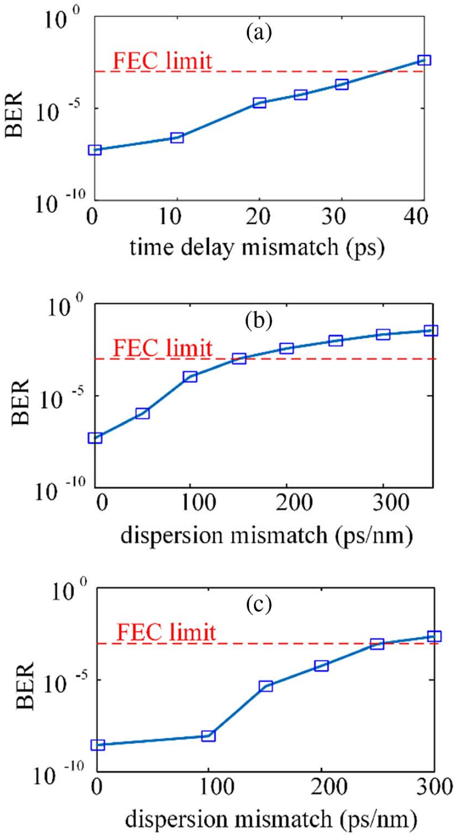

Fig. 4. (a) BER variation of the decrypted signal with time-delay mismatch between DL1 and DL2; (b) BER variation of the decrypted signal with dispersion mismatch between FBG2 and FBG3; (c) BER variation of the decrypted signal with dispersion mismatch between FBG1 and FBG4.

the feed signal exceeds 0.1, the BER tester displays "fail," which indicates that BER is above 0.1 for an unauthorized receiver.

4. DETAILED DISCUSSION

A. Sensitivity of Parameter Mismatch

In real-world communication systems under harsh environments, a mismatch of the parameters is highly probable. It may lead to the degradation of decryption performance. From the security point of view, the sensitivity to the keys is also a great concern.

The parameter sensitivity is evaluated by calculating the BER of the decrypted data when a certain mismatch is intentionally introduced. We consider the three parameters which form the key space, namely, the dispersion of FBG1 (FBG4), FBG2 (FBG3) and the delay time of the SPMF loop. The relationship between the decryption BER and mismatch is plotted in Fig. 4. A BER below 10^{-7} is measured with a 10 ps time-delay mismatch when other parameters are matched. Similar phenomena can be observed with a 100 ps/nm dispersion mismatch between FBG1 and FBG4, or a 10 ps/nm dispersion mismatch between FBG2 and FBG3. These facts indicate that the confidential parameters allow a certain degree of mismatch. On the other hand, BER above 10^{-3} is measured with a 40 ps time-delay mismatch, a 250 ps/nm dispersion mismatch of FBG1, or a 150 ps/nm dispersion mismatch of FBG2. The results imply that parameter mismatches should be controlled within a minimal range. Thus, the legitimate receiver can obtain error-free data after forward error correction (FEC).

From the cryptographical point of view, the parameters can be adjusted with high sensitivity, especially the time delay, which can reach the level of a picosecond. The range of the delay time can be enlarged by adding additional fiber into the SPMF loop, which can provide a large time-domain key space. Moreover, the center wavelength of the FBGs and the overall gain of SPMF can be adjusted and further expand the key space [19,44].

B. Time-Delay Concealment

In the proposed scheme, the secret keys should be the dispersion value of FBGs and the time delay in the SPMF module. Among them, time delay with high parameter sensitivity can provide large key space. The security of a physical layer encryption system rests with the difficulty of cracking secret keys. However, the droppers may calculate the exact time delay through statistical analysis of the transmitted signal. This has also been a serious issue in other schemes, which contain a time-domain key. Thus, it is important that the TDS is properly concealed. A widely used method, autocorrelation function (ACF), is adopted to evaluate the TDS. The function is defined by

$$C(s) = \frac{\langle [v(t) - \langle v(t) \rangle][v(t-s) - \langle v(t) \rangle] \rangle}{[\langle v(t) - \langle v(t) \rangle \rangle]^2}, \tag{6}$$

where $\langle \cdot \rangle$ stands for time average, and $v(t)$ represents the time series of the optical output before the transmission link with a time period of 20 μs.

First, we test the performance of the original system without parameter optimization. The experiment setup is the same as that of the transmitter in Fig. 1. The cumulative dispersions of FBG1 and FBG2 are set as −800 ps/nm and −1200 ps/nm, respectively. As shown in Fig. 5(a), without parameter optimization, the ACF of the time series displays an obvious peak at $t = 99.82$ ns, corresponding to the total delay time of the feedback loop. As a result, the time delay is easy to extract from the ACF peak for the original parameter settings. Then we set the FBG1 and FBG2 with maximum dispersion of −2000 ps/nm. There are no significant peaks in the ACF, as shown in Fig. 5(b). Under such circumstances, the TDS of the SPMF module is effectively concealed.

In addition, the influence of the dispersions on time-delay concealment is discussed in detail. Figure 6(a) shows the peak sizes of ACF at the relevant time delay for different dispersion values of FBG1. Here we set FBG2 as −2000 ps/nm, and scan the dispersion value of FBG1 from 0 to −2000 ps/nm. The result indicates that the peak size decreases gradually with the continuous increase of dispersion. In the range of 0 to −1400 ps/nm, the peaks are distinguishable. The peaks at relevant time delay are suppressed into an invisible value when the dispersion of FBG1 increases to −1600 ps/nm. Figure 6(b) shows the peak sizes of ACF at the relevant time delay for different dispersion values of FBG2 with FBG1 at constant −2000 ps/nm. The result shows that the time-delay peak first increases with the increase of dispersion in the range of 0 to −400 ps/nm and then decreases gradually with the continuous increase of dispersion to −2000 ps/nm. It can be concluded that time-delay concealment can be realized when we set FBG1 below −1600 ps/nm and FBG2 below −2000 ps/nm.

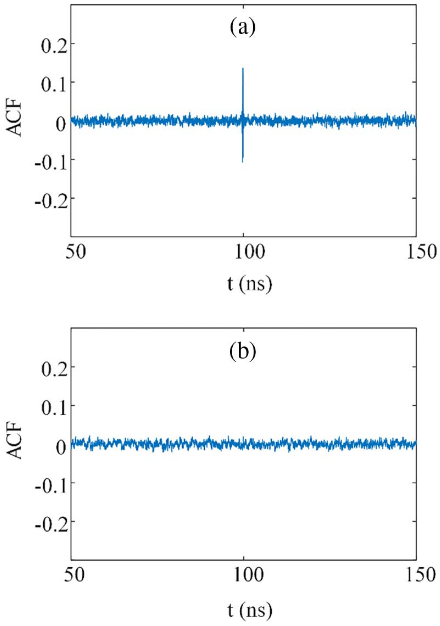

Fig. 5. (a) ACF of time series with original parameter settings; (b) ACF of time series with time-delay concealment.

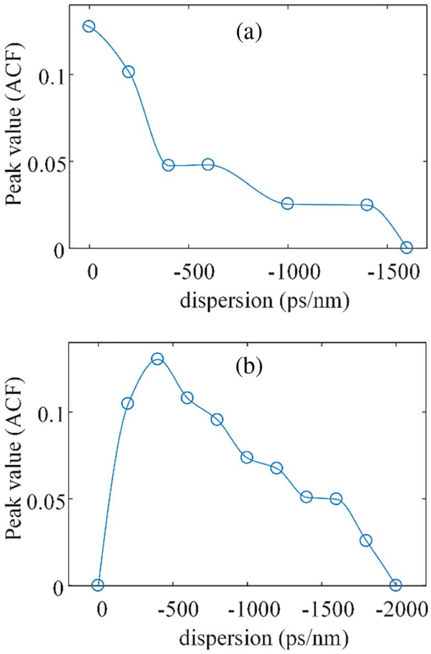

Fig. 6. (a) Peak size of ACF values under different dispersions of FBG1; (b) peak size of ACF values under different dispersions of FBG2.

C. Complexity Analysis

Since complexity is a significant indicator that influences the security of an encryption strategy, it should be discussed and strive to be improved in the scheme. Conceptually, the randomness of a pure noise is higher than that of a chaotic signal. Here we conduct a comparative study.

In order to compare the proposed scheme with a chaotic encryption scheme, we performed a simple experiment about phase chaos first [45]. The experimental setup is shown in Fig. 7(a). It is mainly composed of an electro-optical feedback loop with an FBG to realize PM-to-IM conversion. Here we use permutation entropy (PE) as a quantitative measurement. In this structure, the PE of the output chaos signal is calculated to be 0.9971. Here, 2.5×10^5 points of the output data are used to calculate the PE. In this experiment, the modulation depth of PM is set to be about 2.3. Generally, the modulation depth β is a critical parameter in encryption schemes, especially chaos systems with an electro-optical feedback structure. In a typical electro-optical chaos system, it must be at least 2 [46–48]. In order to obtain a chaos series with higher dynamic complexity, increasing the modulation depth is a common method [49,50]. In these schemes, complexity can reach the level of 0.99 with β above 3. However, high modulation depth may be an obstacle in experimental realization. On the one hand, it greatly relies on devices such as PM with low half-wave voltage and RF with large amplification gain. On the other hand, large modulation depth may lead to difficulties in synchronization and message decryption [3]. Consequently, there is a trade-off between system security and synchronization difficulty.

In order to improve this situation, we introduce an external phase noise source in front of the phase chaos structure, as shown in Fig. 7(b). In this system, the modulation depth of PM2 can dramatically reduce to 0.4 while the complexity remains high. The PE of the output series is calculated to be 0.9979 using 4×10^4 points. We can speculate that the phase noise module mainly contributes to the randomness of the generated signal, since an independent phase-modulated feedback loop cannot even enter the chaotic zone under this parameter setup. These facts indicate that the source of complexity is the external noise, and the SPMF only introduces the time-domain key space.

Since we do not have enough FBGs in the lab, we cannot build a full communication system based on the setup in Fig. 7(b). Therefore, FBG2 is moved out of the feedback loop, and FBG3 is used to compensate for the dispersion induced by FBG2 and the dispersion in the 100 km fiber link simultaneously, as shown in Fig. 1. With this modification, we saved an FBG. In order to quantitatively analyze the complexity of the mask noise, the data source is removed; the experiment setup is shown in Fig. 7(c). The PE of the output signal is calculated to be 0.9972 with 10^5 points. The modulation depths of PM1 and PM2 are calculated to be 0.64 and 0.4, respectively.

These comparisons indicate that introducing an external noise source to a feedback loop structure can maintain high signal complexity with a much lower modulation depth. The implementation difficulty is reduced. In view of the security aspect, the external noise source is also essential for the designed encryption mechanism. If the external noise source is removed, an eavesdropper could use a tunable dispersive medium to compensate for the dispersion of FBG2 and capture the signal by a PD, and then recover the message using the dispersion compensation algorithms in the digital domain. In this case, the loop delay of the SPMF is no longer a secret key, and the security level is degraded.

It is also worth noting that the internal feedback module can be realized in different forms. With the FBG inside the feedback loop [Fig. 7(b)], additional key dimensions, such as the center wavelength of the FBG, can be introduced [19]. However, the structure will be more complex. The trade-off between security and robustness should be taken into account under different circumstances. Other loop structures such as the acousto-optic system [14–17], which could provide several additional keys for security, could also be potentially used in our mechanism. Similarly, the external noise source can be replaced by other broadband entropy sources with high complexity. The structure of the proposed scheme has the potential to be further developed, and different functional parts in our model can be independently designed in a modular manner.

D. DWDM Scenario

Wavelength division multiplexing (WDM) is an effective strategy to expand the capacity for fiber communication. We proposed a DWDM scheme based on our encryption/decryption strategy. The schematic is shown in Fig. 8. Data sources with different wavelengths are multiplexed and encrypted in a common encryptor. Each channel holds an individual receiver to realize data decryption due to the fact that decryption parameters for different wavelengths could be different.

We also performed an experiment to demonstrate the efficiency of the scheme under the DWDM scenario. The channel spacing is set as 0.4 nm (50 GHz), and the central frequencies of two tunable lasers are 193.400 and 193.450 THz, respectively. The IM signal of the two wavelengths is encrypted in a common encryptor. After transmission, a common FBG is used to compensate for the dispersion of FBG2 and fiber link

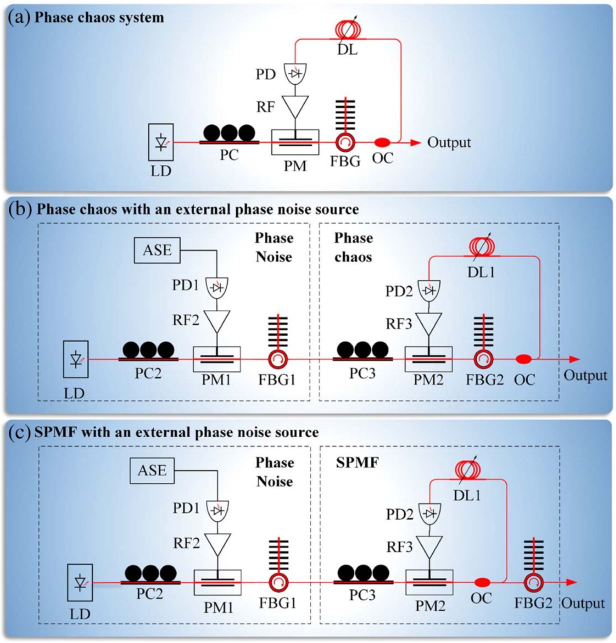

Fig. 7. System structures for complexity measurement. (a) Phase chaos structure; (b) phase chaos with an external phase noise source; (c) SPMF loop with an external phase noise source.

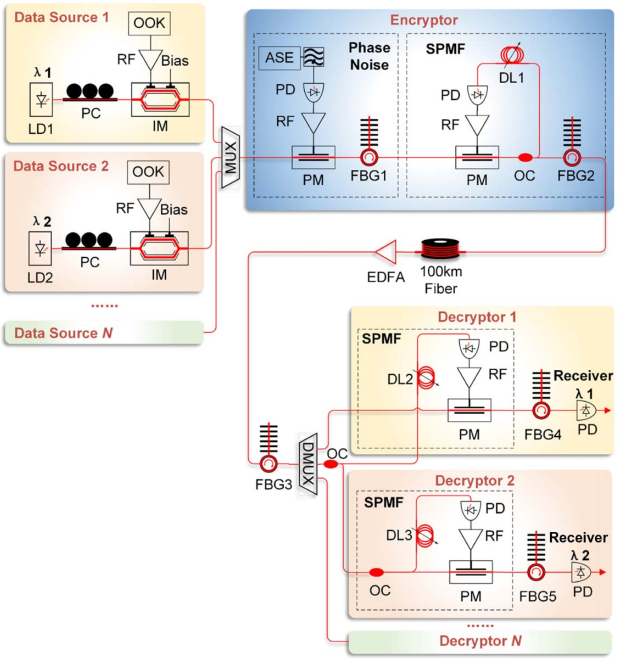

Fig. 8. Experiment structure of the proposed encryption scheme for WDM.

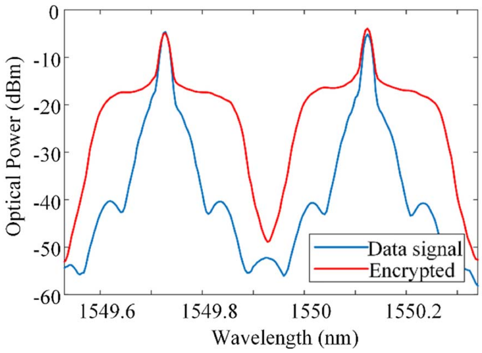

Fig. 9. Spectra of DWDM channels.

for two wavelengths at the same time. Then the signal is demultiplexed and decrypted independently. Due to the lack of devices, we perform the decryption of the two wavelengths successively, with only one set of decryptor and receiver in the experiment. Result shows that DWDM will not affect the normal performance of the secure communication system. The BER performance is similar to that of the single wavelength configuration for both the legitimate receiver and eavesdropper. We also measure the optical domain signal using an optical spectrum analyzer (AQ6370C). The corresponding spectra are shown in Fig. 9. The blue line indicates the original data signal of two channels, and the red line indicates the encrypted signal.

Note that in most of the WDM secure schemes, the encryption and decryption process is mutually independent between channels. The demand for devices multiplies with the increase of wavelength [51,52], while in our scheme, a common encryptor can perform the encryption for different wavelengths simultaneously, which could save costs markedly.

5. CONCLUSION

In this paper, we propose a novel physical layer encryption scheme based on external noise and an internal feedback mechanism. The advantages of external noise source and the feedback loop structure are used synergistically, while their deficiencies are overcome or suppressed. As a result, the IM data are masked by high complexity phase noise, and a robust key space with TDS concealment is established. Based on these facts, optical secure transmission with the rate of 10 Gb/s is successfully realized over 100 km SSMF. The parameter mismatch can be tolerated to a certain degree. However, the stability performance could be affected by environmental factors such as temperature and vibration. This issue could be the major problem that hinders chaotic secure communications in practical applications and will be a focus in our future research. Finally, a compact DWDM scheme with two channels is experimentally demonstrated to show its potential in supporting large-capacity communications.

Funding. National Key R&D Program of China (2018YFB1801304); State Key Laboratory of Advanced Optical Communication Systems and Networks (2019GZKF7); National Natural Science Foundation of China (61505061, 61675083); Key Project of RD Program of Hubei Province (2017AAA046).

REFERENCES

1. B. Wu, B. J. Shastri, and P. R. Prucnal, "Secure communication in fiber-optic networks," in *Emerging Trends in ICT Security*, B. Akhgar and H. Arabnia, eds. (Elsevier, 2014), pp. 173–183.
2. E. Wohlgemuth, Y. Yoffe, T. Yeminy, Z. Zalevsky, and D. Sadot, "Photonic-layer encryption and steganography over IM/DD communication system," Opt. Express **26**, 32691–32703 (2018).
3. R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications," IEEE J. Quantum Electron. **46**, 1430–1435 (2010).
4. K. Tanizawa and F. Futami, "Digital coherent 20-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 800-km SSMF," in *Optical Fiber Communication Conference (OFC)*, OSA Technical Digest (Optical Society of America, 2019), paper Th1J.7.
5. N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," Opt. Lett. **44**, 1536–1539 (2019).
6. B. Wu, M. P. Chang, B. J. Shastri, P. Y. Ma, and P. R. Prucnal, "Dispersion deployment and compensation for optical steganography based on noise," IEEE Photon. Technol. Lett. **28**, 421–424 (2016).
7. B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, "Optical steganography based on amplified spontaneous emission noise," Opt. Express **21**, 2065–2071 (2013).
8. B. Wu, Z. Wang, B. J. Shastri, M. P. Chang, N. A. Frost, and P. R. Prucnal, "Temporal phase mask encrypted optical steganography carried by amplified spontaneous emission noise," Opt. Express **22**, 954–961 (2014).
9. B. Wu, Y. Huang, S. Zhang, B. J. Shastri, and P. R. Prucnal, "Long range secure key distribution over multiple amplified fiber spans based on environmental instabilities," in *Conference on Lasers and Electro-Optics*, OSA Technical Digest (Optical Society of America, 2016), paper SF1F.4.
10. B. Wu, M. P. Chang, B. J. Shastri, Z. Wang, and P. R. Prucnal, "Analog noise protected optical encryption with two-dimensional key space," Opt. Express **22**, 14568–14574 (2014).
11. Q. Yu, Z. Zhao, L. Deng, M. Cheng, M. Zhang, S. Fu, and D. Liu, "Secure optical communication system based on ASE noise with no need for key distribution," in *10th International Conference on Advanced Infocomm Technology* (2018), pp. 47–51.
12. S. Wang, Z. Zou, T. Xing, J. Wang, Z. Wang, and F. Jiang, "Research on optical security based on simulated noise induced encryption scheme," J. Phys. Conf. Ser. **1176**, 062059 (2019).
13. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature **438**, 343–346 (2005).
14. M. R. Chatterjee, A. Mohamed, and F. S. Almehmadi, "Secure free-space communication, turbulence mitigation, and other applications using acousto-optic chaos," Appl. Opt. **57**, C1–C13 (2018).
15. F. S. Almehmadi and M. R. Chatterjee, "Secure chaotic transmission of electrocardiography signals with acousto-optic modulation under profiled beam propagation," Appl. Opt. **54**, 195–203 (2015).
16. F. S. Almehmadi and M. R. Chatterjee, "Improved performance of analog and digital acousto-optic modulation with feedback under profiled beam propagation for secure communication using chaos," Opt. Eng. **53**, 126102 (2014).
17. A. Mohamed and M. R. Chatterjee, "Image intensity recovery with mitigation in the presence of gamma-gamma atmospheric turbulence using encrypted chaos," Opt. Eng. **58**, 036110 (2019).
18. J. Ke, L. Yi, G. Xia, and W. Hu, "Chaotic optical communications over 100-km fiber transmission at 30-Gb/s bit rate," Opt. Lett. **43**, 1323–1326 (2018).
19. D. M. Wang, L. S. Wang, Y. Y. Guo, Y. C. Wang, and A. B. Wang, "Key space enhancement of optical chaos secure communication: chirped FBG feedback semiconductor laser," Opt. Express **27**, 3065–3073 (2019).

20. T. T. Hou, L. L. Yi, X. L. Yang, J. X. Ke, Y. Hu, Q. Yang, P. Zhou, and W. S. Hu, "Maximizing the security of chaotic optical communications," Opt. Express **24**, 23439–23449 (2016).
21. V. S. Udaltsov, J. P. Goedgebuer, L. Larger, J.-B. Cuenot, P. Levy, and W. T. Rhodes, "Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations," Phys. Lett. A **308**, 54–60 (2003).
22. V. S. Udaltsov, L. Larger, J. P. Goedgebuer, A. Locquet, and D. S. Citrin, "Time delay identification in chaotic cryptosystems ruled by delay-differential equations," J. Opt. Technol. **72**, 373–377 (2005).
23. Y. Xua, L. Zhang, P. Lu, S. Mihailov, L. Chen, and X. Bao, "Time-delay signature concealed broadband gain-coupled chaotic laser with fiber random grating induced distributed feedback," Opt. Laser Technol. **109**, 654–658 (2019).
24. P. Xiao, Z. M. Wu, J. G. Wu, L. Jiang, T. Deng, X. Tang, L. Fan, and G. Q. Xia, "Time-delay signature concealment of chaotic output in a vertical-cavity surface-emitting laser with double variable-polarization optical feedback," Opt. Commun. **286**, 339–343 (2013).
25. C. Xue, N. Jiang, G. Li, C. Wang, S. Lin, Y. Lv, and K. Qiu, "Time delay signature suppression and complexity enhancement of chaos in laser with self-phase-modulated optical feedback," in *Conference on Lasers and Electro-Optics*, OSA Technical Digest (online) (Optical Society of America, 2017), paper JTu5A.105.
26. D. Wang, L. Wang, T. Zhao, H. Gao, Y. Wang, X. Chen, and A. Wang, "Time delay signature elimination of chaos in a semiconductor laser by dispersive feedback from a chirped FBG," Opt. Express **25**, 10911–10924 (2017).
27. R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, "Digital key for chaos communication performing time delay concealment," Phys. Rev. Lett. **107**, 034103 (2011).
28. R. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," Opt. Express **20**, 25333–25344 (2012).
29. C. Xue, N. Jiang, Y. Lv, C. Wang, G. Li, S. Lin, and K. Qiu, "Security-enhanced chaos communication with time-delay signature suppression and phase encryption," Opt. Lett. **41**, 3690–3693 (2016).
30. M. Cheng, L. Deng, H. Li, and D. Liu, "Enhanced secure strategy for electro-optic chaotic systems with delayed dynamics by using fractional Fourier transformation," Opt. Express **22**, 5241–5251 (2014).
31. N. Li, W. Pan, A. Locquet, and D. S. Citrin, "Time-delay concealment and complexity enhancement of an external-cavity laser through optical injection," Opt. Lett. **40**, 4416–4419 (2015).
32. P. Mu, W. Pan, L. Yan, B. Luo, N. Li, and M. Xu, "Experimental evidence of time-delay concealment in a DFB laser with dual-chaotic optical injections," IEEE Photon. Technol. Lett. **28**, 131–134 (2016).
33. C. Cheng, Y. Chen, and F. Lin, "Chaos time delay signature suppression and bandwidth enhancement by electrical heterodyning," Opt. Express **23**, 2308–2319 (2015).
34. A. B. Wang, B. J. Wang, L. Li, Y. C. Wang, and K. A. Shore, "Optical heterodyne generation of high-dimensional and broadband white chaos," IEEE J. Sel. Top. Quantum Electron. **21**, 531–540 (2015).
35. J. Wu, Z. Wu, G. Xia, and G. Feng, "Evolution of time delay signature of chaos generated in a mutually delay-coupled semiconductor lasers system," Opt. Express **20**, 1741–1753 (2012).
36. N. Jiang, C. Wang, C. Xue, G. Li, S. Lin, and K. Qiu, "Generation of flat wideband chaos with suppressed time delay signature by using optical time lens," Opt. Express **25**, 14359–14367 (2017).
37. M. Cheng, X. Gao, L. Deng, L. Liu, Y. Deng, S. Fu, M. Zhang, and D. Liu, "Time-delay concealment in a three-dimensional electro-optic chaos system," IEEE Photon. Technol. Lett. **27**, 1030–1033 (2015).
38. A. Zhao, N. Jiang, C. Wang, J. Zhang, and K. Qiu, "Wideband complexity-enhanced optical chaos generation and its application for fast random bit generation," in *CLEO Pacific Rim Conference*, OSA Technical Digest (Optical Society of America, 2018), paper F2D.4.
39. D. Rontani, E. Mercier, D. Wolfersberger, and M. Sciamanna, "Enhanced complexity of optical chaos in a laser diode with phase-conjugate feedback," Opt. Lett. **41**, 4637–4640 (2016).
40. P. Li, Q. Cai, J. Zhang, B. Xu, Y. Liu, A. Bogris, K. A. Shore, and Y. Wang, "Observation of flat chaos generation using an optical feedback multi-mode laser with a band-pass filter," Opt. Express **27**, 17859–17867 (2019).
41. H. Kantz and E. Olbrich, "Coarse grained dynamical entropies: investigation of high-entropic dynamical systems," Physica A **280**, 34–48 (2000).
42. Y. Fu, M. Cheng, X. Jiang, L. Deng, M. Zhang, and D. Liu, "High-speed optical secure communication system using phase modulated random noise," in *10th International Conference on Advanced Infocomm Technology* (2018), pp. 36–40.
43. H. Chi, X. Zou, and J. Yao, "Analytical models for phase-modulation-based microwave photonic systems with phase modulation to intensity modulation conversion using a dispersive device," J. Lightwave Technol. **27**, 511–521 (2009).
44. M. Li, X. Zhang, Y. Hong, Y. Zhang, Y. Shi, and X. Chen, "Confidentiality-enhanced chaotic optical communication system with variable RF amplifier gain," Opt. Express **27**, 25953–25963 (2019).
45. L. Yi, J. Ke, G. Xia, and W. Hu, "Phase chaos generation and security enhancement by introducing fine-controllable dispersion," J. Opt. **20**, 024004 (2018).
46. B. Romeira, F. Kong, W. Li, J. M. L. Figueiredo, J. Javaloyes, and J. Yao, "Broadband chaotic signals and breather oscillations in an optoelectronic oscillator incorporating a microwave photonic filter," J. Lightwave Technol. **32**, 3933–3942 (2014).
47. R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. Udaltsov, and J. Dudley, "Electro-optic delay oscillator with nonlocal nonlinearity: optical phase dynamics, chaos, and synchronization," Phys. Rev. E **80**, 026207 (2009).
48. Q. Li, D. Chen, Q. Bao, R. Zeng, and M. Hu, "Numerical investigations of synchronization and communication based on an electro-optic phase chaos system with concealment of time delay," Appl. Opt. **58**, 1715–1722 (2019).
49. M. Cheng, L. Deng, X. Gao, H. Li, and M. Tang, "Security-enhanced OFDM-PON using hybrid chaotic system," IEEE Photon. Technol. Lett. **27**, 326–329 (2015).
50. C. Wang, Y. Ji, H. Wang, and L. Bai, "Security-enhanced electro-optic feedback phase chaotic system based on nonlinear coupling of two delayed interfering branches," IEEE Photon. J. **10**, 7203415 (2018).
51. Q. C. Zhao and H. X. Yin, "Performance analysis of dense wavelength division multiplexing secure communications with multiple chaotic optical channels," Opt. Commun. **285**, 693–698 (2012).
52. N. Jiang, J. Wang, D. Liu, C. Xue, and K. Qiu, "Secure WDM-PON based on chaos synchronization and subcarrier modulation multiplexing," J. Opt. Soc. Am. B **33**, 637–642 (2016).