Physical Layer Encryption for WDM Optical Communication Systems Using Private Chaotic Phase Scrambling

Anke Zhao, Ning Jiang, *Senior Member, IEEE, Member, OSA*, Shiqin Liu, Yiqun Zhang, and Kun Qiu

***Abstract*—Protecting the security of optical network is a major worldwide challenge. The conventional schemes for securing communications are based on cryptography at the MAC layer and its higher layers, which are facing a great threat with the development of quantum computers. Optical encryption is a promising way for building security on the physical layer of optical communications. In this work, we propose a novel optical encryption scheme for wavelength division multiplexing (WDM) fiber-optic communication systems, by utilizing the private chaotic phase scrambling. Secure transmission of 50 Gbps signal over 50-km standard single-mode fiber is experimentally and numerically demonstrated. The results show that the WDM signal is efficiently encrypted into a noise-like signal, due to the spectral broadening effect of chaotic phase scrambling. Since the processes of encryption and decryption are totally implemented in the optical domain, the proposed scheme can encrypt the entire network traffic with low latency and high speed. Moreover, the proposed encryption scheme is compatible with the existing WDM optical networks, and only one pair of encryption and decryption devices is sufficient to encrypt all WDM channels, thus the scheme can be easily implemented at low hardware cost.**

***Index Terms*—Chaos synchronization, optical encryption, optical fiber communication, physical layer security.**

I. Introduction

OPTICAL fiber communication has been widespread adopted for its advantages of large capacity and long transmission distance in various applications including personal, commercial and military communications. With the increasing demand for network capacity, the issue of securing optical network is becoming increasingly important [1], [2]. As with other network types, traditional ways for securing optical network are done by employing cryptographic protocols at the MAC layer and its higher layers of the protocol stack. However, conventional cryptographic schemes are facing a major treat as the development of quantum computers, which have the potential to crack the ciphers in a short period of time. Thus, it is desirable to build security at the physical layer of optical network and resist attacks that might target this layer. Encryption on the physical layer of optical communication systems also enables data signals to be encrypted with high speed and low latency [1].

Several optical encryption schemes have been proposed by the optical communications community over the years, such as optical XOR logic [3], [4], optical steganography [5], optical code division multiplexing (OCDMA) [6] and spectral phase encryption with dispersive components [7], [8]. These schemes can effectively improve the privacy and security of the data signals, but they still have several disadvantages. In the encryption process of optical XOR logic, another data sequence is required for encrypting the transmitted data using XOR logic. The encrypted data can be recorded and recovered by employing post-processing decryption, since it remains in digital form. Regarding to optical steganography, the stability of data decryption might be affected by the sensitive interference structure. Besides, the security of optical steganography has a potential risk, since the time delay might be identified by an illegal receiver with several statistical methods [9]. OCDMA techniques are implemented by overlapping multiple channels in the same frequency space, however, the practical security of this kind of encryption scheme is still an open issue [6]. Spectral phase encryption requires dispersive devices for achieving phase-to-intensity conversion, the nonlinearity effect of dispersion may affect its performance of long haul optical fiber transmission.

Optical chaos encryption is another scheme for providing optical layer security, which has been widely studied in the past two decades [10]–[12]. By employing broadband chaos as the optical carrier, optical chaos encryption can convert the transmitted data as a noise-like signal [13]. Without eliminating the chaotic carrier from the received optical signal, the eavesdropper is unable to recover the data. However, the practical applications of optical chaos encryption are also limited by two aspect: one is that the complexity of chaotic carrier affects the security of chaos-based systems [14]–[17]; the other is that the bandwidth of chaotic carrier limits the data rate. Although methods have been reported for enhancing the bandwidth of the chaotic carrier [18]–[23], synchronization and communication using bandwidth-enhanced chaos are still challenging. In addition, wavelength division multiplexing (WDM) technology is one of key technologies to increase the speed and capacity of

Manuscript received November 1, 2020; revised December 16, 2020; accepted January 9, 2021. Date of publication January 13, 2021; date of current version April 16, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 61671119 and Grant 61805031, in part by the Sichuan Science and Technology Program under Grant 2021JDJQ0023, in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2019J003, and in part by STCSM under Grant SKLSFO2020-05. *(Corresponding author: Ning Jiang.)*

The authors are with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: ab_zhao@163.com; uestc_nj@uestc.edu.cn; liushiqinlsq@163.com; zhangyiqun2019@163.com; kqiu@uestc.edu.cn).

Color versions of one or more of the figures in this article are available online at https://doi.org/10.1109/JLT.2021.3051407.

Digital Object Identifier 10.1109/JLT.2021.3051407

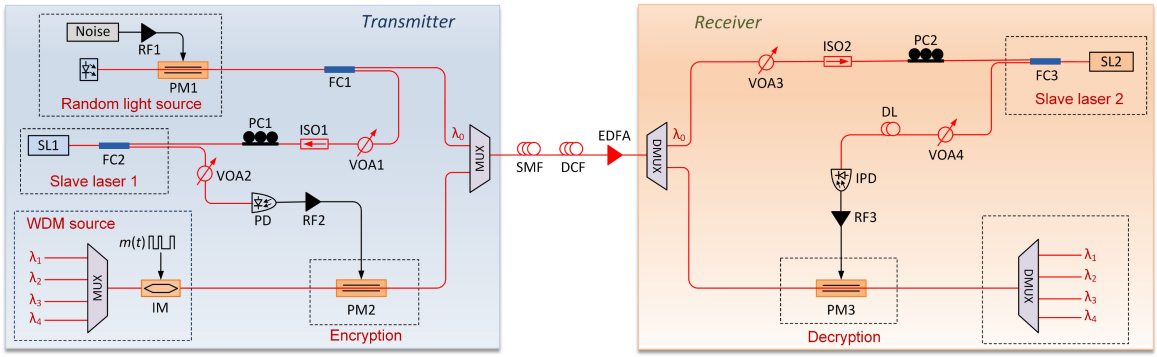

Fig. 1. Experimental setup of the proposed secure WDM optical communication system. SL, slave semiconductor laser; PC, polarization controller; PM, electro-optical phase modulator; FC, fiber coupler; RF: radio-frequency amplifier; ISO, optical isolator; (I)PD: (inverse) photodetector; VOA, variable optical attenuator; IM, intensity modulator; DL, variable optical delay line; SMF, standard single-mode fiber; DCF, dispersion compensating fiber; EDFA, erbium doped fiber amplifier.

optical fiber communications. However, the practical application of the above mentioned optical encryption schemes in WDM optical communication systems still needs further explorations.

In this paper, we propose and demonstrate a new optical layer encryption scheme for WDM fiber-optic communication systems, in virtue of the private chaotic phase scrambling. The proposed scheme is implemented optically and realized on the optical layer, which can encrypt the entire network traffic with low latency and high speed. In contrast with the optical chaos encryption, in this scheme, the chaotic signals are utilized as the driving signals rather than the optical carrier, thus the transmission capacity is no longer limited by the bandwidth of chaotic signals. Moreover, our encryption scheme is compatible with and can be directly added to the existing WDM optical network, which opens an alternative route in secure optical communication.

II. Experimental Setup

In Fig. 1, we present the schematic diagram of the proposed secure WDM optical communication system. We assemble the encryption and decryption schemes on a typical WDM optical communication system. At the transmitter, four continuous-wave (CW) lasers with a linewidth of 100 kHz are used as the light sources, which are wavelength-multiplexed onto a single fiber and then intensity modulated by a 12.5 Gbps non-return-to-zero on-off keying (NRZ-OOK) signal. The channel spacing is set to 0.3 nm, and the central wavelengths of these four channels are $\lambda_1 = 1549.3$ nm, $\lambda_2 = 1549.6$ nm, $\lambda_3 = 1549.9$ nm and $\lambda_4 = 1550.2$ nm, respectively. The WDM signal is then sent to an electro-optical phase modulator (PM2) for encryption. After transmission, the encrypted WDM signal is sent to another phase modulator (PM3) at the receiver for decryption. The encrypted signal is transmitted over a standard 50-km single-mode fiber (SMF), then a dispersion compensation fiber (DCF) with a dispersion value of 816 ps/nm is used to compensate the dispersion of SMF and an erbium-doped fiber amplifier (EDFA) is utilized to compensate the transmission loss. Two private chaotic signals are utilized as the driving signals of PM2 and PM3, which are obtained from two local slave semiconductor lasers (SL1 and SL2) subject to common injection of a constant-amplitude random-phase (CARP) light. The CARP light is emitted by another CW laser with a central wavelength of $\lambda_0 = 1550.9$ nm. The output of the CW laser is phase modulated by a Gaussian noise signal which is generated by a 25 GS/s arbitrary waveform generator (AWG). The CARP light is split into two beams by a 50:50 fiber coupler (FC1): one beam is injected to SL1, and the other beam is wavelength-multiplexed with the encrypted WDM signal. At the receiver, a wavelength selective switch (WSS) is used to separate the CARP signal from the encrypted WDM signal. Then the filtered CARP light is injected into SL2, and the filtered encrypted WDM signal is sent to PM3. Here the amplitude of the driving signal of PM2 is opposite with that of the driving signal of PM3. The decrypted WDM signal is then de-multiplexed by a variable optical filter, and detected by photo-detectors (PDs). In our system, the CARP light and the encrypted WDM signal are transmitted through a single optical fiber, the same transmission distance ensures the transmission delays of these two signals are identical. Moreover, we use a variable optical delay line at the receiver to further eliminate the synchronization error. Therefore, the synchronization between the two chaotic signals used to drive PM2 and PM3 can be maintained. In our experiment, the SLs are two distributed-feedback (DFB) lasers. The operation wavelengths of both SL1 and SL2 are set to 1550.85 nm, and their emission powers are set to 0 dBm. The optical injection powers of SL1 and SL2 are set as -5dBm. The PDs have a bandwidth of 30 GHz. The PMs have a bandwidth of 20 GHz and a half-wave voltage of 3.8 V. The PM modulation depth of PM1 is about 1, and those of PM2 and PM3 are about 2. The maximum power gains of the RF amplifies are 38 dB with a frequency range of 0.5 to 18 GHz. We use a 4-channel 25-GHz digital oscilloscope to measure and record the electronic signals, and its real-time sampling rate is set as 100 GS/s. An optical spectrum analyzer with a resolution of 0.03 nm is used to measure the optical signals.

III. Experimental Results and Discussions

First, we investigate the encryption performance in the proposed secure communication system. In Fig. 2, we present the

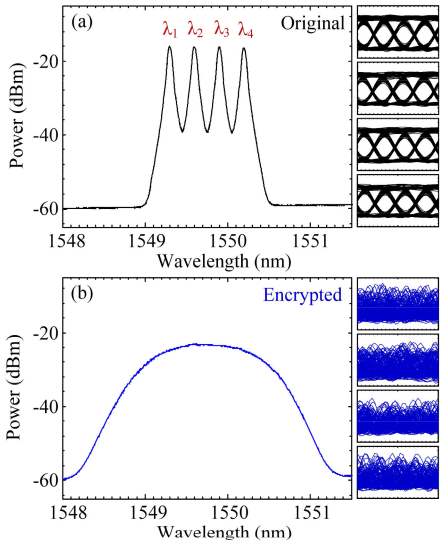

Fig. 2. Experimental optical spectra of (a) the original WDM signal and (b) the encrypted WDM signal, as well as the corresponding eye diagrams of the four channels.

optical spectra of the original WDM signal and the encrypted WDM signal, as well as the eye diagrams of the four channels. The optical spectrum of the original WDM signal is significantly extended and becomes exceptionally flat after the encryption, which is attributed to that the phase-modulation of chaotic signal causes spectral broadening effect and degrades the signal-to-noise ratio. Since each channel is significantly overlapped with its adjacent channels, the receiver cannot directly implement channel isolation by a demultiplexer without the decryption. Besides, the information about the central wavelengths and channel spacing is concealed in the optical spectrum. It has been demonstrated that the physical layer of optical communication systems is vulnerable to several kinds of attacks [1]. Here we assume a possible scenario for eavesdropping where the eavesdropper has known the information including the central wavelengths, the bit rates and the modulation formats of all channels (even they are well hidden). Then he separates these four channels with the known central wavelengths, and recovers the messages with the corresponding bit rates and modulation formats. As can be seen in Fig. 2(b), the eye diagrams of all the channels obtained by the eavesdropper are completely closed, and the corresponding bit error rates (BERs) are around 0.4. We also compare the temporal waveforms and the power spectra of the original NRZ signal and the encrypted signal as shown in Fig. 3. Here we choose the channel λ_1 to display the results. It can be seen that after the encryption, the temporal waveform is greatly distorted and the power spectrum is obviously flattened, which indicates that the data is well buried into a noise-like signal.

In our system, the encryption performance is mainly affected by the modulation depth of PM2. In Fig. 4, we illustrate the optical spectra of the encrypted signals with different modulation depths. As shown in Figs. 4(a) and 4(b), the spectra are relatively flat when the modulation depths are set to 2 and 1.7. However, when the modulation depths are reduced to 1.4 and 1.1,

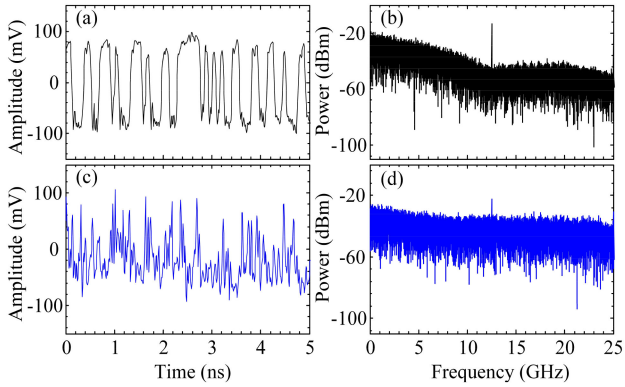

Fig. 3. Temporal waveforms (first column) and power spectra (second column) of (a), (b) the original NRZ signal and (c), (d) the encrypted signal of channel λ_1.

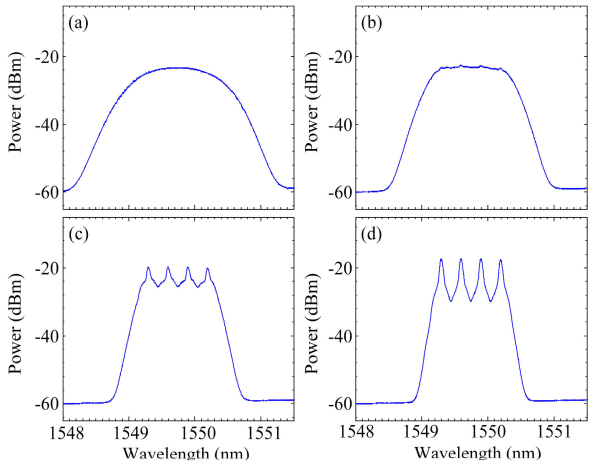

Fig. 4. Optical spectra of the encrypted signals with the modulation depths of (a) 2, (b) 1.7, (c) 1.4, and (d) 1.1.

all the four channels are distinguishable and the corresponding optical signal-to-noise ratios are obviously increased as shown in Figs. 4(c) and 4(d). It is indicated that the larger the PM modulation depth, the better the encryption performance is.

We adopt BER to quantify the influence of PM modulation depth on the encryption performance, the BERs of the encrypted signals of the four channels are shown in Fig. 5. Here 1.25×10^6 bits are used to calculate the BERs. With the modulation depth increasing, the BERs of all the four channels significantly increase until a stable level ($\sim$0.5). In particular, when the modulation depths are larger than 1.2, the BERs are higher than the hard decision forward error correction (HD-FEC) threshold (3.8×10^{-3}). Therefore, the PM modulation depth should be large enough (at least larger than 1.2) to ensure the successful encryption.

Next, we investigate the decryption performance of our system. In Fig. 6, we present the optical spectra and the eye diagrams of the decrypted WDM signal in the back-to-back situation and the decrypted WDM signal after 50-km transmission. As shown in Fig. 6(a), the overlapped channels are separated from each other after the decryption, and all the four channel signals are correctly recovered with a widely opened eye diagram. We also

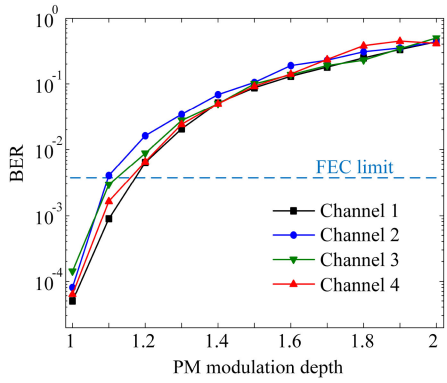

Fig. 5. The influence of PM modulation depth on the BERs of the encrypted signals of the four channels.

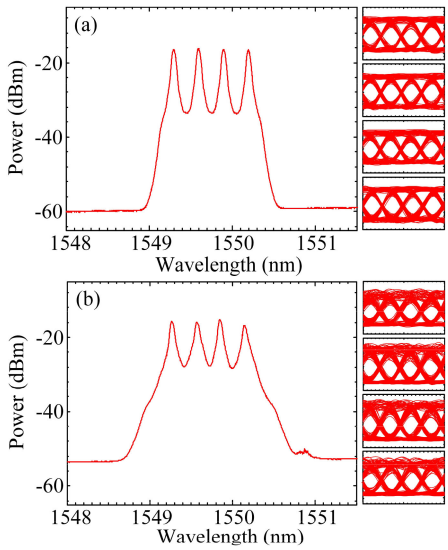

Fig. 6. Experimental optical spectra of (a) the decrypted WDM signal in back-to-back situation and (b) the decrypted signal after 50-km transmission, as well as the corresponding eye diagrams of the four channels.

evaluate our system in 50-km transmission case. As shown in Fig. 6(b), the eye diagrams show that the four NRZ-OOK signals are successfully recovered, and the corresponding BERs of these four signals are lower than 10^{-5}. The above results indicate that, successful decryption can be achieved for the legal receiver with a low BER, and the proposed encryption scheme can protect the data signal from being recovered by the illegal receiver.

In our system, two synchronized chaotic signals are used as the driving signals of PM2 and PM3 for encryption and decryption. In order to ensure the privacy of these two driving signals, they are generated by two local SLs with a common CARP injection [24], [25]. The temporal waveforms of the CARP signal and the output signals of the SLs, as well as the corresponding correlation plots among them are shown in Fig. 7. The CARP signal in Fig. 7(a) shows only a small intensity oscillation which is caused by the noise of the electronic devices. While in Figs. 7(b) and 7(c), due to the injection locking and the phase-modulation to intensity-modulation induced by the low-filtering effect of SLs, the temporal waveforms of SL1 and SL2 exhibit almost the same

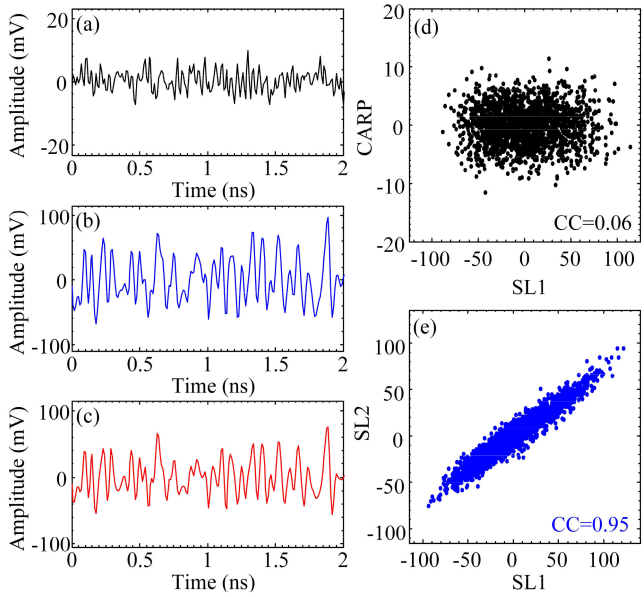

Fig. 7. Temporal waveforms of (a) the common injection signal, and the output signals of (b) SL1 and (c) SL2; as well as the correlation plots between (d) the common injection signal and SL1, and (e) SL1 and SL2.

fluctuations with large amplitudes. The intensity fluctuations of SL1 and SL2 are completely different from that of the CARP signal, and the correlation plot in Fig. 7(d) shows that the CARP signal is not synchronized with the output of SL1 (as well as that of SL2). Comparatively, the correlation plot in Fig. 7(e) shows SL1 and SL2 are well synchronized with each other. We adopt the correlation coefficient (CC) to evaluate the synchronization performance, which is defined as [11]:

$$CC = \frac{\langle (I_1(t) - \langle I_1(t)\rangle) \cdot (I_2(t) - \langle I_2(t)\rangle)\rangle}{\sqrt{\left\langle (I_1(t) - \langle I_1(t)\rangle)^2 \right\rangle \left\langle (I_2(t) - \langle I_2(t)\rangle)^2 \right\rangle}}, \quad (1)$$

where $I_1(t)$ and $I_2(t)$ are the experimental intensity time series, and $<\cdot>$ is the time averaging. 4×10^6 data points which correspond to a length of 40 μs are used to calculate the correlation coefficient. Here the correlation coefficient is calculated from the back-to-back scenario. A large CC value of 0.95 is achieved between the two SLs, indicating a high-quality synchronization of the chaotic signals. While the CC value between the CARP signal and the SLs is only 0.06, which indicates that no synchronization is achieved among them. In our system, only the common injection light is required to be transmitted over the public link, thus the privacy of the locally generated chaotic signals can be ensured. Moreover, the CARP injection light is combined with the encrypted WDM signal and transmitted through a single fiber, thus, no additional fiber link is required to transmit the common injection light. Moreover, our system only needs one encryption device at the transmitter and one decryption device at the receiver for all channels with different wavelengths, therefore the cost can be considerably reduced. In addition, the encryption and decryption devices can be directly added to existing WDM optical systems without replacing any hardware such as the light source, the amplifiers, transmitters or

receivers, indicating that our encryption scheme is suitable for modern fiber-optic communication systems.

IV. Theoretical Model and Numerical Results

In order to study the proposed encryption scheme more thoroughly and systematically, we also perform numerical investigations and present the simulation results in this section. The dynamics of the SLs in the proposed scheme are described by the modified Lang-Kobayashi rate equations [26], [27], which can be written as

$$\frac{dE(t)}{dt} = \frac{1}{2}(1+i\alpha)[G(t) - \frac{1}{\tau_p}]E(t) + \sigma E_{inj}(t) + \sqrt{2\beta N(t)}\chi(t), \quad (2)$$

$$\frac{dN(t)}{dt} = \frac{I}{q} - \frac{N(t)}{\tau_e} - G(t)|E(t)|^2, \quad (3)$$

$$G(t) = \frac{g[N(t) - N_0]}{1 + \varepsilon|E(t)|^2}, \quad (4)$$

where E is the complex electric field amplitude, and N is the corresponding carrier number. A white Gaussian noise χ with zero mean and unity variance is used to model the spontaneous emission noise. The values of the intrinsic parameters of SL1 and SL2 are chosen as those in [22], [27]: the gain saturation coefficient $\varepsilon = 5 \times 10^{-7}$, the linewidth enhancement factor $\alpha = 5$, the photon lifetime $\tau_p = 2$ ps, the carrier lifetime $\tau_e = 2$ ns, the differential gain parameter $g = 1.5 \times 10^{-8}$ ps^{-1}, the spontaneous emission rate $\beta = 1.5 \times 10^{-6}$ ns^{-1}, and the transparent carrier number $N_0 = 1.5 \times 10^8$. The operation current of the SLs is set as $I = 1.5I_{th}$, where I_{th} is the threshold current which is set as 14.7 mA. $E_{inj}(t)$ is the injection signal of SLs, and σ is the corresponding injection strength which is set to 50 ns^{-1}. The output signal of the PMs can be written as

$$E_{out}(t) = E_{in}(t) \cdot \exp[i\varphi(t)], \quad (5)$$

$$\varphi(t) = K_{PM} \cdot \mathrm{N}[|E(t)|^2] \cdot \pi, \quad (6)$$

where E_{in} and E_{out} are the input and output of phase modulator, respectively. $\varphi(t)$ denotes the phase-shift of the phase modulation, wherein K_{PM} is the modulation depth, N$[|E(t)|^2]$ represents the normalized electronic driving signal. The modulation depth of PM1 is set as 1, and those of PM2 and PM3 are set as 2. In the simulation, the BER is evaluated by [28], [29]

$$BER = \frac{\exp(-Q^2/2)}{\sqrt{2\pi}Q}, \quad (7)$$

where Q is the Q-factor of received message, which is defined as

$$Q = \frac{I_1 - I_0}{\sigma_1 + \sigma_0}, \quad (8)$$

where I_1 and I_0 are the average power of bits "1" and "0", respectively; σ_1 and σ_0 are their standard deviations. For the sake of consistence, the central wavelengths and the bit rates of all the channels are set as the same with those in the experiment. 50-km standard SMF is also chosen as the transmission link, then a DCF and an EDFA are used to compensate the dispersion of SMF and the transmission loss, respectively.

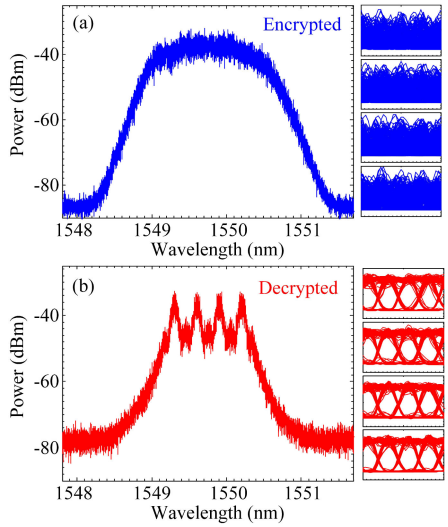

Fig. 8. Numerical optical spectra of (a) the encrypted WDM signal and (b) the decrypted WDM signal, as well as the corresponding eye diagrams of the four channels.

Figure 8 presents the numerical results of the encrypted WDM signal and the decrypted WDM signal. As presented in Fig. 8(a), the optical spectrum becomes considerably flat after the encryption, all the channels are completely overlapped with each other. The eye diagrams of the four channel signals are completely closed, and the corresponding BERs are calculated as higher than 0.3. Thus, the eavesdropper cannot directly recover the data signals using channel isolation with a demultiplexer, even if he knows the central wavelengths, the bit rates and the modulation formats of all the channels. As presented in Fig. 8(b), the original WDM signal is successfully decrypted at the receiver. All the channel signals are well recovered with widely opened eye diagrams, and the BERs of them are lower than 10^{-8}. The results of simulation are consistent with those of experiment, which further indicate that the proposed scheme can achieve secure transmission for WDM signals.

Furthermore, the influences of channel spacing and modulation depth of PM1 on the encryption performance are illustrated in Fig. 9. As shown in Fig. 9(a), with the channel spacing increases, the BERs of the encrypted signals of all the channels gradually decrease. The BERs are lower than 3.8×10^{-3} when the channel spacing is larger than 70 GHz (approximately 6 times the data rate). It is indicated that efficient encryption can be achieved in the proposed scheme with a wide range of the channel spacing. Particularly, the BERs of the encrypted signals of all the channels is higher than 0.1 when the channel spacing is smaller than 40 GHz (approximately 3 times the data rate). Therefore, the proposed scheme is rather suitable for solving the security challenges in dense WDM (DWDM) optical communication systems. As shown in Fig. 9(b), the BERs of all the four channels quickly increase to 0.5 as the modulation depth of PM1 increases, the BERs are larger than 3.8×10^{-3} when the modulation depth is larger than 0.2. In our system, the

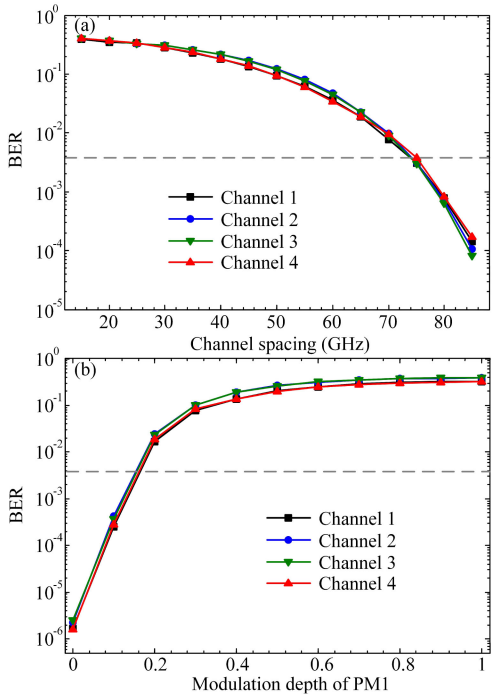

Fig. 9. The BERs of the encrypted signals of the four channels as a function of (a) channel spacing and (b) modulation depth of PM1. The dash line is the threshold of HD-FEC.

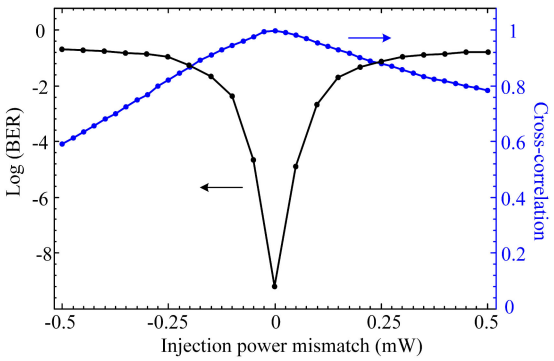

Fig. 10. The influence of injection power mismatch on the cross-correlation between SL1 and SL2 and the BER of the recovered signal.

modulation depth of PM1 is set as 1, which is lager enough to achieve efficient encryption for all the channels.

Since the driving signals at the transmitter and the receiver are two synchronized chaotic signals, their synchronization quality affects the decryption performance. In Fig. 10, we present the influence of synchronization quality on the BER of the decrypted signal. The variation of synchronization quality is controlled by adjusting the mismatch of injection powers between SL1 and SL2. Here, we choose the channel λ_1 to present the results for the sake of simplicity, since the results of other channels are similar. The results show that, the BER of the recovered signal gradually increases as the synchronization quality degrades, which indicates that the imperfect synchronization between the two chaotic signals would affect the decryption performance. When the cross-correlation coefficient is larger than 0.9, the

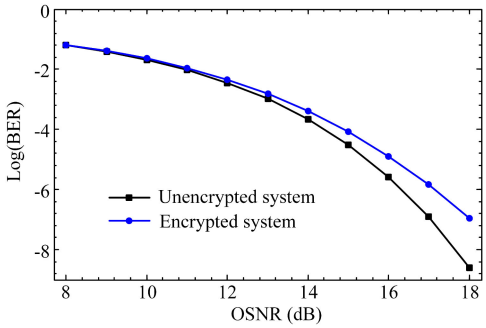

Fig. 11. The influence of optical signal-to-noise ratio (OSNR) on the BER of the original unencrypted system and the encrypted system.

BER can be smaller than 3.8×10^{-3}. Therefore, the high-quality synchronization between the two chaotic driving signals ensures the successful decryption in the proposed scheme. The BER of the recovered signal is sensitive to the parameter mismatch, and good communication performance can be achieved when the parameters of SL1 and SL2 are well matched. In practice, the sensitivity of parameter mismatch is highly related to the security of communication systems. From the security point of view, the parameters should be adjusted with high sensitivity to ensure a large key space.

In Fig. 11, we investigate the comparison of the BER performance between the original unencrypted system and the encrypted system. The results show that, the proposed encryption scheme slightly degrades the transmission performance. As the OSNR increases, the BER of the unencrypted system decreases faster than that of the encrypted system. In practical communication circumstance, the devices used for encryption and decryption cannot perfectly match, and the devices noise affects the synchronization quality between the two chaotic driving signals, thus this degradation is inevitable. However, when taking 3.8×10^{-3} as the threshold, the degradation of optical signal-to-noise ratio (OSNR) is less than 0.3 dB which is within an acceptable range.

To further verify the practicability and feasibility of the proposed optical encryption scheme, we evaluate the proposed scheme in a WDM system with different modulation formats. Here three WDM channels with a channel spacing of 40 GHz are considered, including a 20 Gbps NRZ-OOK channel, a 40 Gbps QPSK channel and an 80 Gbps 16-QAM channel. Figure 12 presents the optical spectra of the encrypted and decrypted WDM signals. The eye diagram of the NRZ-OOK signal and the constellations of the QPSK and 16-QAM signals are also illustrated. As shown in Fig. 12(a), the chaotic phase modulation greatly flattens the optical spectrum and degrades the signal-to-noise ratio. The eye diagram and constellations of the encrypted signals are completely noisy. While for the legal receiver as shown in Fig. 12(b), all the channel signals are correctly recovered, and the corresponding eye diagram and constellations can be recognized.

Figure 13 presents the influence of modulation depth of PM2 on the BERs of the encrypted signals of these three channels. As the modulation depth increases, the BERs of all these channels

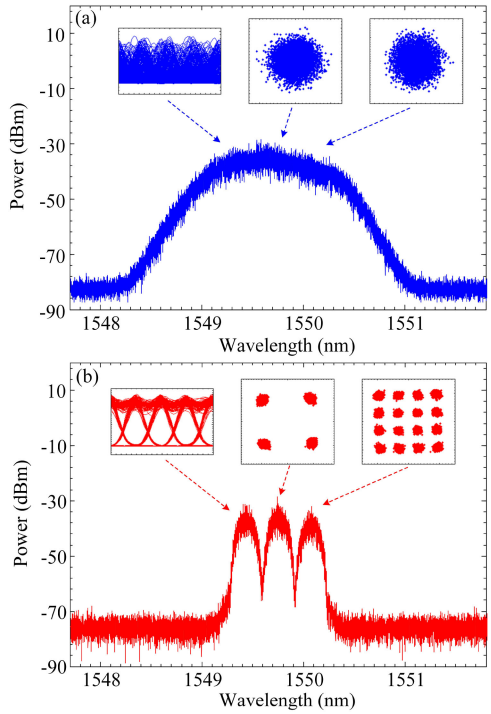

Fig. 12. Optical spectra of (a) the encrypted WDM signal and (b) the decrypted WDM signal. The three channels are 20 Gbps NRZ-OOK signal, 40 Gbps QPSK signal and 80 Gbps 16-QAM signal, respectively, with a channel spacing of 40 GHz. The insets are the corresponding eye diagram and constellations of the three channel signals.

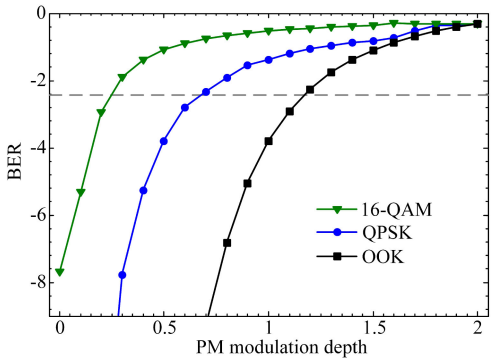

Fig. 13. The BERs of the encrypted signals of the three channels as a function of modulation depth of PM2.

quickly increase until a stable level of around 0.5. The thresholds of modulation depth for the NRZ-OOK channel, the QPSK channel and the 16-QAM channel are 0.3, 0.7 and 1.2, respectively. For the QPSK and 16-QAM signals, only a small modulation depth can achieve phase scrambling, thus the thresholds of these two channels are smaller than that of the NRZ-OOK channel. It can be concluded that, the proposed encryption scheme is compatible with WDM systems with different modulation formats. Moreover, when the PM modulation depth is large enough, only one encryption module is sufficient to encrypt all the channels.

V. Conclusion

We proposed a novel secure WDM optical communication scheme with the temporal encryption and decryption of chaotic phase scrambling. 4 $\times$ 12.5 Gbps secure transmission over a standard 50-km SMF were experimentally and numerically demonstrated. The conditions of PM modulation depth and channel spacing were investigated for achieving efficient encryption. The results indicate that, successful encryption can be achieved with a BER higher than 0.3, which protects the data signal from being recovered by the illegal receiver. While successful decryption can be achieved for the legal receiver with a BER lower than 10^{-5}. In our scheme, a common-signal-induced synchronization configuration is utilized to distribute the chaotic driving signals, thus the privacy of the chaotic signals can be ensured. Moreover, the proposed optical encryption scheme is compatible with and can be directly added into the existing WDM/DWDM optical networks with different modulation formats and data rates. The proposed scheme opens a new pathway for protecting the security of optical WDM communication systems.

References

[1] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 725–736, Sep. 2011.
[2] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.
[3] Z. Li and G. Li, "Ultrahigh-speed reconfigurable logic gates based on four-wave mixing in a semiconductor optical amplifier," *IEEE Photon. Technol. Lett.*, vol. 18, no. 12, pp. 1341–1343, Jun. 2006.
[4] Y. Liu, F. Qin, Z. M. Meng, F. Zhou, Q.-H. Mao, and Z.-Y. Li, "All-optical logic gates based on two-dimensional low-refractive-index nonlinear photonic crystal slabs," *Opt. Express*, vol. 19, no. 3, pp. 1945–1953, 2011.
[5] 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*, vol. 22, no. 1, pp. 954–961, Jan. 2014.
[6] Z. Jiang, D. E. Leaird, and A. M. Weiner, ''Experimental investigation of security issues in O-CDMA," *J. Lightw. Technol.*, vol. 24, no. 11, pp. 4228–4234, Nov. 2006.
[7] X. Wang, Z. Gao, N. Kataoka, and N. Wada, "Time domain spectral phase encoding/DPSK data modulation using single phase modulator for OCDMA application," *Opt. Express*, vol. 18, no. 10. pp. 9879–9890, Apr. 2010.
[8] 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.*, vol. 44, no. 7, pp. 1536–1539, Apr. 2019.
[9] 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.*, Mar. 2019, Art. no. 062059.
[10] A. Argyris *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 17, pp. 343–346, Nov. 2005.
[11] 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.*, vol. 43, no. 6, pp. 1323–1326, Mar. 2018.
[12] X. Gao, M. Cheng, L. Deng, M. Zhang, S. Fu, and D. Liu, "Robust chaotic-shift-keying scheme based on electro-optical hybrid feedback system," *Opt. Express*, vol. 28, no. 8, pp. 10847–10858, Apr. 2020.
[13] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nat. Photon.*, vol. 9, no. 3, pp. 151–162, Mar. 2015.
[14] D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, and S. Ortin, "Time-delay identification in a chaotic semiconductor laser with optical feedback: A dynamical point of view," *IEEE J. Quantum Electron.*, vol. 45, no. 7, pp. 879–891, Jul. 2009.

[15] 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.*, vol. 40, no. 19, pp. 4416–4419, Oct. 2015.
[16] Y. Fu *et al.*, "High-speed optical secure communication with an external noise source and an internal time-delayed feedback loop," *Photon. Res.*, vol. 7, no. 11, pp. 1306–1313, Nov. 2019.
[17] S. Y. Xiang *et al.*, "Wideband unpredictability-enhanced chaotic semiconductor lasers with dual-chaotic optical injections," *IEEE J. Quantum Electron.*, vol. 48, no. 8, pp. 1069–1076, Aug. 2012.
[18] A. Wang, B. Wang, L. Li, Y. Wang, and K. A. Shore, "Optical heterodyne generation of high-dimensional and broadband white chaos," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 6, pp. 531–540, Nov./Dec. 2015.
[19] Y. H. Hong, P. S. Spencer, and K. A. Shore, "Wideband chaos with time-delay concealment in vertical-cavity surface-emitting lasers with optical feedback and injection," *IEEE J. Quantum Electron.*, vol. 50, no. 5, pp. 236–242, Apr. 2014.
[20] N. Jiang, A. K. Zhao, S. Q. Liu, C. P. Xue, B. Y. Wang, and K. Qiu, "Generation of broadband chaos with perfect time delay signature suppression by using self-phase-modulated feedback and a microsphere resonator," *Opt. Lett.*, vol. 43, no. 21, pp. 5359–5362, Nov. 2018.
[21] A. K. Zhao, N. Jiang, S. Q. Liu, C. P. Xue, and K. Qiu, "Wideband time delay signature-suppressed chaos generation using self-phase-modulated feedback semiconductor laser cascaded with dispersive component," *J. Lightw. Technol.*, vol. 37, no. 19, pp. 5132–5139, Oct. 2019.
[22] A. K. Zhao, N. Jiang, S. Q. Liu, C. P. Xue, J. M. Tang, and K. Qiu, "Wideband complex-enhanced chaos generation using a semiconductor laser subject to delay-interfered self-phase-modulated feedback," *Opt. Express*, vol. 27, no. 9, pp. 12336–12348, Apr. 2019.
[23] M. Cheng *et al.*, "An electrooptic chaotic system based on a hybrid feedback loop," *J. Lightw. Technol.*, vol. 36, no. 19. pp. 4259–4266, Oct. 2018.
[24] K. Yoshimura *et al.*, "Secure key distribution using correlated randomness in lasers driven by common random light," *Phys. Rev. Lett.*, vol. 108, no. 7, Feb. 2012, Art. no. 070602.
[25] A. K. Zhao, N. Jiang, S. Q. Liu, Y. Q. Zhang, and K. Qiu, "Generation of synchronized wideband complex signals and its application in secure optical communication," *Opt. Express*, vol. 28, no. 16, pp. 23363–23373, Aug. 2020.
[26] R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," *IEEE J. Quantum Electron.*, vol. 16, no. 3, pp. 347–355, Mar. 1980.
[27] N. Li, W. Pan, L. Yan, B. Luo, X. Zou, and S. Xiang, "Enhanced two-channel optical chaotic communication using isochronous synchronization," *IEEE J. Sel. Top. Quantum Electron.*, vol. 19, no. 4, Jul./Aug. 2013, Art. no. 0600109.
[28] F. Zhang and P. L. Chu, "Effect of transmission fiber on chaotic communication system based on erbium-doped fiber ring laser," *J. Lightw. Technol.*, vol. 21, no. 12, pp. 3334–3343, Dec. 2003.
[29] A. Bogris, D. Kanakidis, A. Argyris, and D. Syvridis, "Performance characterization of a closed-loop chaotic communication system including fiber transmission in dispersion shifted fi bers," *IEEE J. Quantum Electron.*, vol. 41, no. 3, pp. 1326–1336, Mar. 2005.

Anke Zhao was born in Sichuan, China, in 1992. He received the B.Eng. degree in 2016 from the University of Electronic Science and Technology of China, Chengdu, China, where he is currently working toward the Ph.D. degree. His research interests include the nonlinear dynamics of semiconductor lasers, secure optical communication, and secure key distribution.

Ning Jiang (Senior Member, IEEE) was born in Sichuan, China, in 1984. He received the B.S. degree in communication engineering from the University of Electronic Science and Technology, Chengdu, China, in 2005 and the Ph.D. degree in communication and information system from Southwest Jiaotong University, Chengdu, China, in 2012. He is currently a Professor with the School of Information and Communication Engineering, University of Electronic Science and Technology, Chengdu, China. He has authored or coauthored more than 90 research papers. His current research interests include all-optical secure communication and energy-efficient optical access network. He is also a member of the Optical Society of America, and a reviewer of the IEEE PHOTONICS TECHNOLOGY LETTERS, the *Optics Express*, the *Optics Letters*, the *Journal of Lightwave Technology*, the IEEE JOURNAL OF QUANTUM ELECTRON, the IEEE PHOTONICS JOURNAL, the *Applied Optics*, *Optics Communications*, and some other journals.

Shiqin Liu was born in Sichuan, China, in 1995. She received the B.S. degree from Southwest University, Chongqing, China, in 2017. She is currently working toward the Ph.D. degree with the University of Electronic Science and Technology of China, Chengdu, China. Her research interests include the complex chaos network.

Yiqun Zhang was born in Henan, China, in 1997. He received the B.Eng. degree from Xidian University, Xi'an, China, and Heriot-Watt University, Edinburgh, U.K., in 2019. He is currently working toward the Ph.D. degree with the University of Electronic Science and Technology of China, Chengdu, China. His research interests include the optical chaotic communications.

Kun Qiu received the M.S. and Ph.D. degrees from Tsinghua University, Beijing, China, in 1987 and 1990, respectively. In 1990, he joined the University of Electronic Science and Technology of China, Chengdu, China, where he was involved in the theories and technologies in optical fiber communications. From 1993 to 1994, he was a Visiting Scholar with the Institution of Optics, University of Rochester, Rochester, NY, USA. From 2002 to 2006, he was the Director of the State Key Laboratory of the Broadband Optical Transmission and Communication Network. He has finished more than 20 important projects as a Research Team Leader. He has authored or coauthored more than 200 scientific papers and the book of *Optical Fiber Communication*. He was the recipient of eight awards of science and technology progress from provinces or ministries. He was the Chair of the Chengdu Chapter and the IEEE Photonics Society.