



# Research on the Performance of Multimode Optical Chaotic Secure Communication System With Multidimensional Keys and a Complex Entropy Source

Jingyang Liu , Xuefang Zhou , and Weihao Chen

**Abstract**—In this paper, we design an optical chaotic secure communication system with multi-dimensional keys and a complex entropy source, which can allow secure communication working in different modes such as unicast, multicast, and broadcast. In the proposed scheme, amplified spontaneous emission (ASE) noise of the erbium-doped fiber amplifier (EDFA) with sufficient randomness is used as an entropy source to improve the security of the system. And by using the electro-optic delay feedback loops, the key spaces are introduced and the phase distortion is generated, then the data are masked in both phase and intensity fields. As a frequency-dependent group delay (FDGD) module, Gires-Tournois interferometer (G-T I) in the feedback loop can effectively hide the time delay signature (TDS) and achieve additional  $10^{36}$  key spaces. The influence of different key mismatches on decryption function is numerically investigated, and the results indicate that the broadband nature of ASE noise makes the TDS a very sensitive encryption key, which increases the difficulty of illegal third parties stealing information. And with the help of the wavelength converter and wavelength division multiplexer, secure communication in various modes is successfully realized, which greatly improves the communication efficiency and is suitable for various security places.

**Index Terms**—Chaos, secure communication, amplified spontaneous emission, frequency-dependent group delay.

## I. INTRODUCTION

ALTHOUGH chaotic secure communication system has been considered a good candidate system to provide information security, due to the noise-like, broadband, and unpredictable characteristics of chaotic signals, the security of chaotic communication systems is still an urgent problem to be solved.

Manuscript received 23 June 2022; revised 23 July 2022; accepted 28 July 2022. Date of publication 2 August 2022; date of current version 22 August 2022. This work was supported in part by the Natural Science Foundation of China under Grant 61705055, in part by the Zhejiang Province Key Research and Development Project in 2020 under Grant 2019C01G1121168, and in part by the Zhejiang Province Science and Technology Plan Projects under Grant LGG19F050001. (Corresponding author: Xuefang Zhou.)

Jingyang Liu and Weihao Chen are with the School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China (e-mail: 905995272@qq.com; 1009065819@qq.com).

Xuefang Zhou is with the School of cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China, and also with the School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China (e-mail: zhouxf@hdu.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2022.3195750

Based on the basic work of Pérez and Cerdeira [1], researchers believed that the security of the chaotic communication system can be improved by using higher-dimensional chaotic carriers. However, this is not entirely true. High-dimensional chaotic carriers can indeed improve the security of the system, but more importantly, whether the system can prevent the illegal third party from revealing their basic parameters when the illegal third party is independent of the dynamic behavior of the chaotic system. If the illegal third party can infer the values of each parameter in the system, such as modulation intensity, offset phase, time delay signature (TDS), etc., then the illegal third party can reconstruct chaotic dynamics and build an illegal receiver to steal information. Among these parameters, the range of modulation intensity and offset phase is narrow, and the parameter information can be extracted by trial and error [2]. For the TDS, the third party can use the delay time identification technology such as auto-correlation function (ACF), delay mutual information (DMI) [3], [4], and permutation entropy (PE) [5], deep learning [6] to extract the TDS. Therefore, aiming to improve the security of the chaotic secure communication system, it is necessary to hide TDS, which is the critical security key of the chaotic system.

Many methods have been proposed to hide TDS, one method is based on the all-optical feedback loop. Rontani D et al. proposed that the TDS can be selected to be close to the relaxation oscillation period of the laser, and the laser can be in a medium feedback state, which can hide the TDS effectively in 2007 [7]. Four years later, the Nguimdo R M team obtained the corresponding TDS by detecting the optical phase auto-correlation characteristics, which denied the effectiveness of the above method [8]. Subsequently, Nguimdo R M [9] team proposed a scheme by using cross-feedback semiconductor ring lasers in 2012 to hide TDS, and successfully eliminated the intensity and phase TDS based on using cross-feedback between reverse propagation modes in bidirectional semiconductor ring lasers. In addition, researchers also found that semiconductor lasers are very sensitive to external disturbances. When the semiconductor laser is disturbed by the injection from another laser [10], the feedback from a distant mirror [10], [11], the chaotic optical injection [12], and the injection of the self-feedback loop [13], the lasers may output broadband chaos without TDS. Another

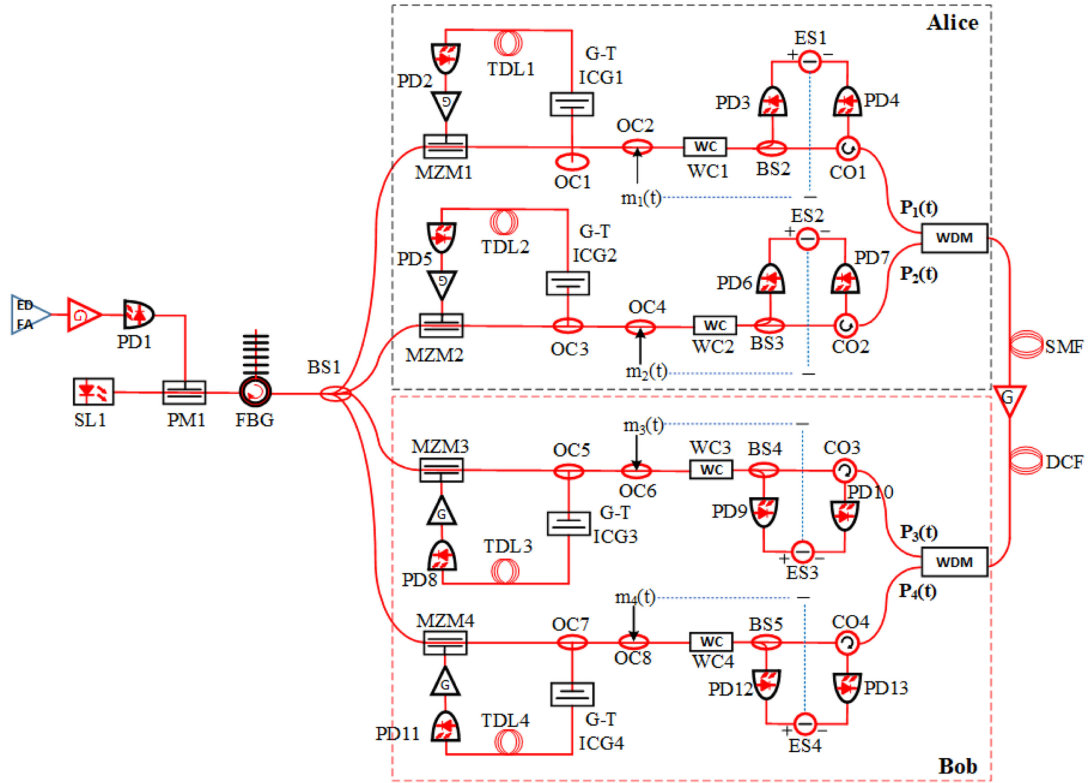


Fig. 1. The schematic diagram of the multimode optical chaotic secure communication system ( $N = 2$ ).

method is based on electro-optic feedback. The Nguimdo R M team firstly demonstrated that the complexity of chaos can be improved and the TDS can be suppressed by using the parallel or serial structure of the dual electro-optic feedback loops [14], [15]. In the electro-optic feedback loop parallel system, the internal TDS can be effectively hidden by using the internal loop dynamics characteristics independent of the encrypted signal. In 2016, Hou T T et al. introduced the FDGD module in the chaotic feedback loop as the hardware key to hide the TDS [16], whose advantage is that the TDS can be hidden without increasing the system complexity.

To enhance the security of chaotic communication systems, another idea is increasing the complexity of chaos. In 2010, J. Hizanidis et al. combined all-optical and electro-optical schemes [17] and injected the intensity chaotic carrier into the electro-optical delay feedback loop to enhance the complexity of chaotic signals. Furthermore, double masking [18] and gain variation [19] also were used to enhance the complexity of chaos.

Therefore, from two aspects of increasing chaotic complexity and hiding TDS, we propose a multi-mode optical chaotic secure communication system with a multi-dimensional key and complex entropy source based on ASE noise source. In secure communication, ASE noise is often used as an ultra-wideband entropy source [20], [21] to provide a wider bandwidth. Moreover, as a real noise signal, the randomness of ASE noise is much higher than that of a noise-like chaotic signal [22]. ASE noise sources can enhance system security. And the dispersion-induced characteristics of fiber Bragg grating (FBG) and the electro-optic delay feedback loop are used to realize the double

masking in the phase and intensity fields. The Gires–Tournois interferometer cascade group (G-T ICG) is introduced into the electro-optic delay feedback loop to increase the complexity of the system under the premise of effectively hiding TDS. On this basis, the system can realize communication in different modes at the same time by combining wavelength converter with wavelength division multiplexing scene.

## II. SYSTEM ARCHITECTURE

The architecture of the multimode chaotic secure communication is illustrated in Fig. 1. In this scheme, Alice and Bob consist of  $N$  transmitters, respectively. The transmitters in Alice can transmit the messages with the transmitters in Bob with different modes such as unicast, multicast, or broadcast. By adjusting wavelength converters' state, different communication modes can be achieved. Unicast: adjust any transmitter of Alice and Bob with the same wavelength to realize one-to-one bidirectional communication. Multicast: adjust any transmitter in Alice and multiple transmitters in Bob with the same wavelength to realize one-to-many unidirectional communication. Broadcast: adjust any transmitter in Alice and all transmitters in Bob to achieve one-to-all unidirectional communication. Similarly, the multicast and broadcast modes of Bob to Alice can also be realized. As long as the transmitters working in different modes are ensured to be at different wavelengths, secure communication in various modes can be realized at the same time.

Taking the simplest unicast mode as an example, we select any transmitter in Alice and Bob to describe the principle of

TABLE I  
IDEALLY, THE DIGITAL DEMONSTRATION OF DECRYPTION STEPS.  
(THE SYMBOLS IN THE TABLE CORRESPOND TO FIG. 1.)

Alice		Bob	
$m_1(t)$	1 1 0 1 0	$m_3(t)$	0 1 0 1 0
$P_1(t)-P_3(t)$	1 0 0 0 0	$P_3(t)-P_1(t)$	-1 0 0 0 0
$m_1(t)-(P_1(t)-P_3(t))$	0 1 0 1 0	$m_3(t)-(P_1(t)-P_3(t))$	1 1 0 1 0

system encryption and decryption messages. Firstly, the ASE noise is loaded on the optical carrier with a central frequency of 193.1THz through a phase modulator (PM), the output of PM is used as the entropy source of the system, and FBG is used to realize the phase modulation to intensity modulation (PM-to-IM) conversion. Next, the beam splitter (BS) divides the optical wave into 2N channels (the former N channels belong to Alice, and the latter N channels belong to Bob). In the transmitter of Alice, a separated signal is fed into an electro-optical Mach-Zehnder modulator (MZM). The output enters G-T ICG which can make different frequency signals produce different degrees of group delay and is transmitted through a tunable delay line (TDL). The collocation of G-T ICG and TDL greatly increases the key space. TDL output signal is detected with a photodetector (PD), the converted electrical signal is amplified by an amplifier, and the resulting output voltage drives the input of the MZM, closing thus the feedback loop. Through the optical coupler, the double masking of chaotic carrier on the phase and intensity of information is achieved. The encrypted message is divided into two paths by BS, one is left locally, and the other is transmitted to the transmitter of Bob through the circulator(CO) and the wavelength division multiplexer(WDM). The encryption principle of Bob is the same as that of Alice, and will not be repeated here. We use  $P_i(t)(i \in [1, N])$  and  $P_j(t)(j \in [N+1, 2N])$  respectively to represent the power of encrypted signals generated at the transmitters of Alice and Bob. Therefore, the end in Alice can receive the synchronization power error  $P_i(t)-P_j(t)$  of two encrypted messages. Similarly, the end in Bob receives  $P_j(t)-P_i(t)$ . Finally, by subtracting the received synchronization power error from the local signal, the message on the other end can be recovered to realize one-to-one bidirectional transmission. The specific message exchange processes are shown in Table I.

Among them, the G-T ICG is composed of multiple G-T Is. G-T I is an optical interferometer composed of two parallel mirrors [23]. The front mirror is partial reflection, and the rear mirror is full reflection. The air gap between the two mirrors constitutes a G-T cavity. The optical wave is incident from the front mirror, and the reflection occurs continuously in the cavity, resulting in multi-beam interference, which changes the phase, path, and time delay of the optical wave. The optical path difference  $\Delta$  and phase difference  $\delta$  of two adjacent beams are respectively:

$$\Delta = 2n'd \cos \theta \quad (1)$$

$$\delta = \frac{4\pi}{\lambda} n'd \cos \theta \quad (2)$$

Where  $n'$  and  $d$  is the refractive index and cavity length of the cavity medium,  $\lambda$  and  $\theta$  is the incident optical wavelength and incidence angle. Using  $k$  to number of the G-T I in the G-T ICG in order, where the G-T ICG with  $k = 6$  is selected, the group delay  $\tau_k(\omega)$  of the  $k$ -th G-T I at different wavelengths is:

$$\tau_k(\omega) = \frac{2n'_k d_k \cos \delta_k}{c} \frac{1 - r_k}{2\sqrt{r_k} \cos \delta_k - (1 + r_k)} \quad (3)$$

$r$  is the reflection coefficient of the front mirror,  $c$  is the speed of light. Then, the group delay of G-T ICG module is:

$$\tau(\omega) = \sum_{k=1}^6 \tau_k(\omega) \quad (4)$$

The ASE noise is modulated by a semiconductor laser(SL) with a central wavelength of 1550nm and a power of 0dBm. The output signal [24] of PM is:

$$E_1(t) = E_0(t) \cdot \exp\left(j \cdot \frac{\pi}{V_\pi} \cdot ASE(t)\right) \quad (5)$$

$E_0(t)$  is the output signal of SL, and  $V_\pi$  is the half-wave voltage. The output signal of PM continues to pass through FBG. The dispersion transfer function  $H(f)$  of FBG is:

$$H(f) = \exp\left(-2\pi j \int \tau_{FBG}(f) df\right) \quad (6)$$

$\tau_{FBG}(f)$  is the group delay of FBG, which is determined by the central wavelength  $\lambda_c$ , bandwidth  $\Delta_\lambda$ , and cumulative dispersion  $D$ :

$$\tau_{FBG}(\lambda) = \begin{cases} \tau_0 & \lambda \leq \lambda_c - \Delta_\lambda/2 \\ D \cdot \lambda & \lambda_c - \Delta_\lambda/2 < \lambda \leq \Delta_\lambda/2 \\ \tau_{\lambda_c} + \Delta_\lambda/2 & \lambda > \lambda_c + \Delta_\lambda/2 \end{cases} \quad (7)$$

The output light wave of FBG is:

$$E(t) = \text{ifft}\{\text{fft}[E_1(t)]H(f)\} \quad (8)$$

Subsequently, BS divides the light into 2N paths and light enters the electro-optic delay feedback loops. Inspired by the study of nonlinear delay dynamics in optics by Ikeda [25], it is assumed that the chaotic dynamics in the electro-optic delay feedback loop are dominated by a linear filter, which is characterized by a high cut-off time related to  $\gamma$  and a low cut-off time related to  $\theta$ .  $G$  is the feedback strength, which is determined by the photoelectric conversion efficiency, amplification gain, and optical input power in the feedback loop. The calculation formula is as follows:  $G = \pi\eta ASP_0/(2V_\pi)$ ,  $\eta$  is the total light damage in the loop,  $A$  is the amplification gain, and  $S$  is the photoelectric conversion efficiency of PD,  $V_\pi$  which represents the half-wave voltage of MZM. Referring to the reference [14]–[17], [27], the dynamic mathematical model of the chaotic communication system can be described by the delay integral-differential equations:

$$\begin{aligned} V_i(t) + \gamma_i \frac{dV_i(t)}{dt} + \frac{1}{\theta_i} \int_{t_0}^t V_i(\varepsilon) d\varepsilon \\ = G_i \cos^2 \left[ \frac{1}{2n} E(t - \tau_i(\omega) - \delta T_i) + \phi_i \right] \end{aligned} \quad (9)$$

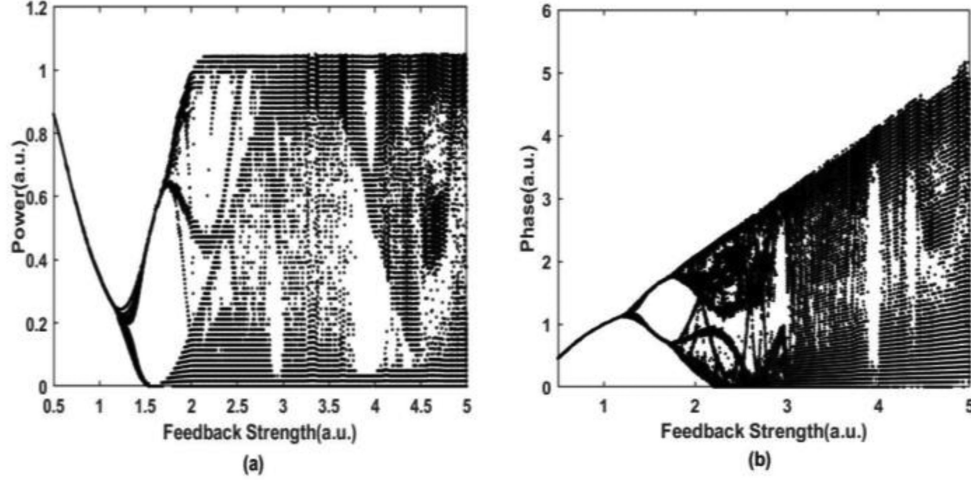


Fig. 2. (a) Intensity chaotic bifurcation diagram; (b) Phase chaotic bifurcation diagram.

$$\begin{aligned}
 V_j(t) + \gamma_j \frac{dV_j(t)}{dt} + \frac{1}{\theta_j} \int_{t_0}^t V_j(\varepsilon) d\varepsilon \\
 = G_j \cos^2 \left[ \frac{1}{2n} E(t - \tau_j(\omega) - \delta T_j) + \phi_j \right] \quad (10)
 \end{aligned}$$

The sub-indices  $i, j$  refer to the transmitters in Alice and Bob, where  $\phi$  is the offset phase of MZM,  $\delta T$  is the TDS generated by TDL.  $\tau(\omega)$  is group delay generated by G-T ICG. Only in the case of perfect matching ( $\theta_i = \theta_j$ ,  $\gamma_i = \gamma_j$ ,  $G_i = G_j$ ,  $\tau_i(\omega) = \tau_j(\omega)$ ,  $\delta T_i = \delta T_j$ ,  $\phi_i = \phi_j$ ), the two ends of the communication will be fully synchronized to effectively realize the encryption and decryption of messages. In Eqs. (9, 10), there is a certain order of magnitude relationship between the high and low cut-off time:  $\theta \approx 10^6 \gamma$ ,  $\tau(\omega) + \delta T$  can be adjusted between  $\theta$  and  $\gamma$ , and its span can reach up to six orders of magnitudes. For the convenience of analysis, all transmitters in Alice and Bob have the same parameters. The parameters are designed according to the experimental accessibility [14], [17], [26]:

$$G_{i,j} = 3.2, \delta T_{i,j} = 500\text{ns}, \gamma_{i,j} = 25\text{ns}, \theta_{i,j} = 5\text{ms}, \phi_{i,j} = -\pi/4.$$

### III. COMPLEXITY AND SECURITY

Since each transmitter in Section II adopts the same parameters, we select any transmitter and plot the intensity and phase chaotic bifurcation diagram related to the feedback strength  $G$  at this transmitter. As can be seen from Fig. 2, with the increase of  $G$ , the system gradually passes through the stable state, the period-doubling state, and finally develops into the chaotic state. High feedback strength can bring high complexity chaotic sequences, but the higher the feedback strength of the communication system isn't the better. Excessive feedback strength will lead to poor synchronization and difficult decryption of the system [22]. And too small feedback strength cannot make the system in a chaotic state. So the feedback strength should be weighed.

In the second section, we refer to the experimentally accessible value and select the feedback strength of the system as 3.2. In general, the feedback strength value of the system is at least

2, 3.2 is a moderate feedback strength value, and will not affect the system decryption ability. And in Fig. 2, the intensity and phase of the light wave generated by the system have entered the chaotic state when  $G = 3.2$ .

The above content can prove that the system is in a chaotic state. Therefore, we now analyze the performance of TDS concealment. As mentioned earlier, the G-T ICG, acting as the FDGD module, can cause different frequency components of the chaotic signal to experience different time delays, and can disturb the complexity of chaotic sequences. By simulation, the group delay curve introduced by G-T ICG is shown in Fig. 3(a). To verify the security of the system, the standard delay time identification techniques are induced to extract the TDS, such as ACF  $A(s)$ ,  $A(s)$ , which is robust to noise perturbation and is suitable to crack the time delay in practical situations [15].

In the absence of G-T ICG, a peak in the ACF curve (as shown in Fig. 3(b)) can be observed at the time delay  $\delta T_{i,j}$  ( $\delta T_{i,j} = 500\text{ns}$ ), which means that the TDS can be extracted from the time series of chaos in the absence of G-T ICG through  $A(s)$ . After adding the G-T ICG, the peak at  $t = 0.5\mu\text{s}$  disappears obviously, and the TDS has been well concealed. The results show that the G-T ICG can hide TDS effectively.

On this basis, different numbers of G-T Is in the loop are discussed to simulate the evolution of TDS contained in the ACF curve, as displayed in Fig. 4. With the increase of the cascade number, the pulse of the ACF curve disappears, and the ACF curve becomes smoother, and the TDS has been well concealed. Furthermore, with an increase in the cascade number, the TDS almost cannot be extracted, so the illegal third party cannot reconstruct chaotic dynamics, which ensures the security of communication. In addition, other modules with FDGD characteristics can be used instead of G-T ICG to achieve the same TDS concealment effect.

### IV. SENSITIVITY OF PARAMETER MISMATCH

Optical chaotic secure communication is a kind of hardware encryption based on a physical layer [27], [28]. In the system,

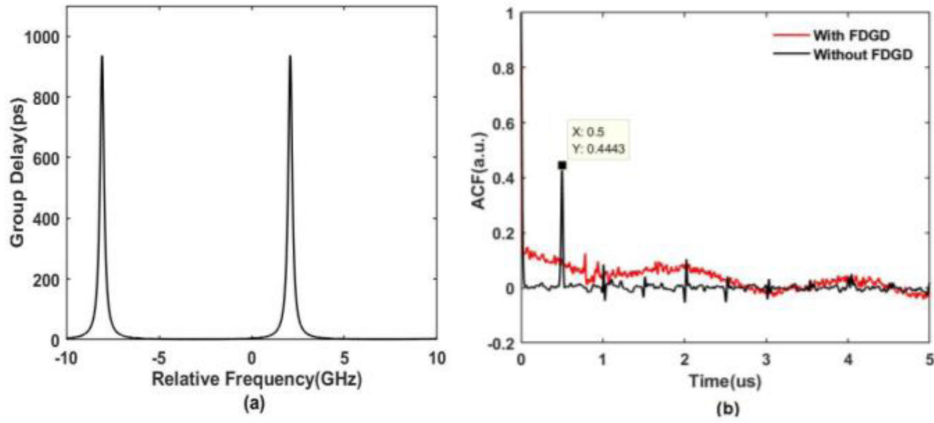


Fig. 3. (a) Group delay curve of a G-T I; (b) ACF curve.

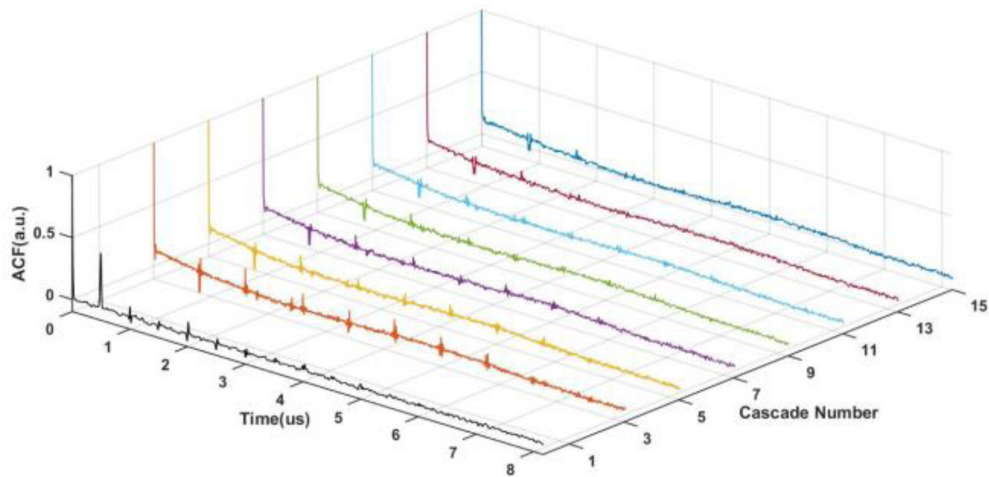


Fig. 4. ACF with various cascade numbers.

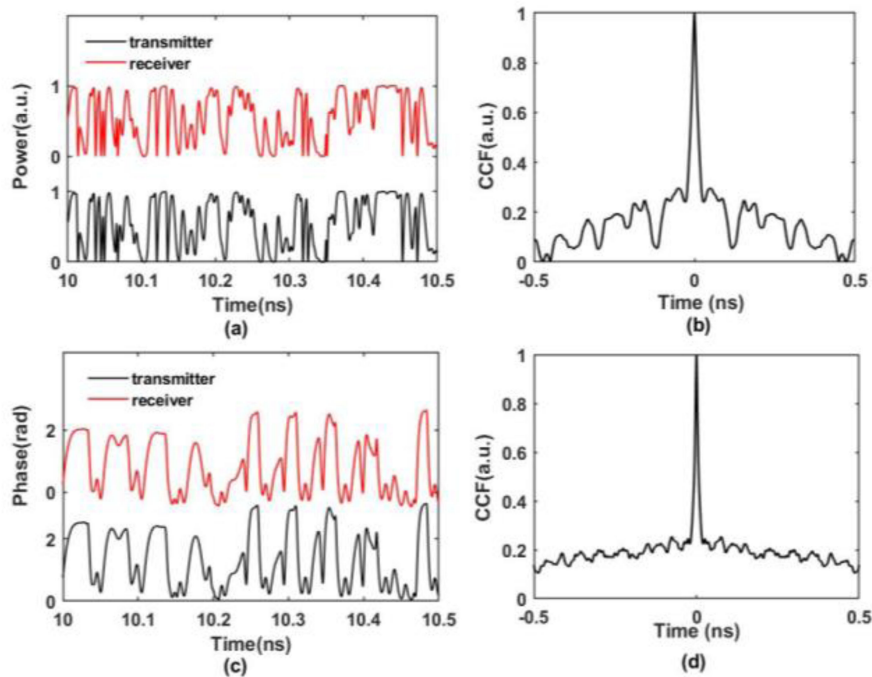


Fig. 5. (a) The optical power curves at both ends; (b) The CCF of the optical power at both ends; (c) The optical phase curves at both ends; (d) The CCF of the optical phase at both ends.

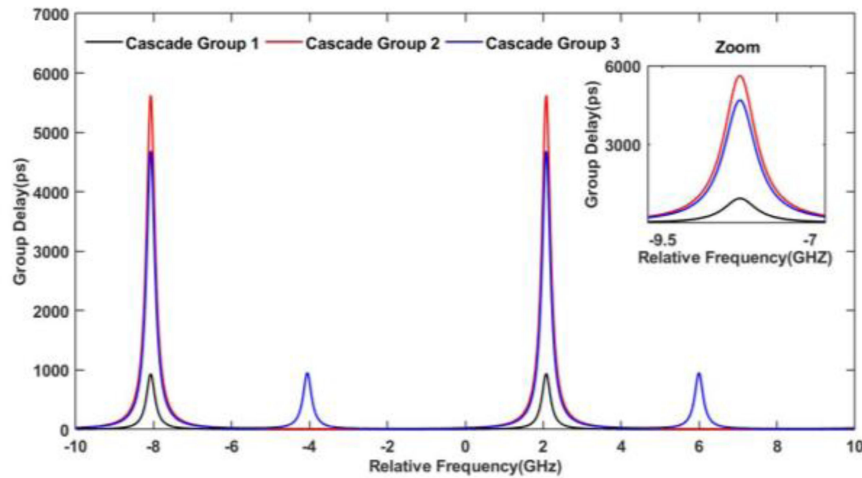


Fig. 6. Group delay curves under different G-T ICGs.

some hardware parameters exist as keys. The sensitivity of these keys is an important index of system security. Low sensitivity means that the key has strong fault tolerance, which will lead to a sharp decline in the confidentiality of the system. The key sensitivity is evaluated by calculating the cross-correlation function (CCF) of chaotic waveforms at both ends of communication when a certain mismatch is intentionally introduced [29].

Here, we consider the three-dimensional parameters which form the key space, namely, the cascade number of the G-T ICG, the cavity length of each G-T I, and the TDS of TDL. In nature, chaos synchronization quality is fundamental in determining the decryption BER [30]. Only when the CCF of chaotic waveforms at both ends of communication is not less than 0.9, the system can perform encryption and decryption with high quality. Therefore, we take 0.9 as the threshold to test the sensitivity of the three-dimensional keys. To simplify the steps, the following operations are carried out in the unicast mode.

Firstly, in the case of no message and perfect matching of parameters at both ends, the synchronization degree of chaotic waveforms is verified. As shown in Fig. 5(a) and (c), the optical power and phase at both ends are shown within 10ns-10.5ns, respectively. From these figures, we find that waveforms at both ends have the same trend in this period. And the CCF of optical power and phase in all periods at both ends is plotted, as shown in Fig. 5(b) and (d). Only when  $t = 0$ , the CCF is 1. It is proved that the synchronization at both ends is a universal phenomenon rather than a special phenomenon in a certain period, that is, the system has synchronization.

Then, by changing the number and cavity length of G-T Is at an end, the effect of FDGD module mismatch on system security is observed. The essence of G-T Is number and cavity length mismatch is the mismatch of the group delay curve. By simulation, the group delay curves under different G-T ICGs are plotted, as shown in Fig. 6. Cascade Group1 is composed of a G-T I with a cavity length of 5cm; Cascade Group2 is composed of six G-T Is with a cavity length of 5cm; Cascade Group3 is composed of five G-T Is with a cavity length of 5 cm and a G-T I with a cavity length of 5.05 cm. There is the cascade number mismatch between Cascade Group1 and Cascade Group2, which is reflected in the multiple relationships

of amplitude between the group delay curves. Cascade Group2 and Cascade Group3 are mismatches of the cavity length and cascade number. The mismatch of cavity length is reflected in different numbers of group delay pulses at different frequencies. Therefore, when constructing the G-T ICG, we can use the combination of interferometers with different cavity lengths to increase the complexity of the group delay curve and improve the security of the system.

We use one G-T I at the transmitter of Alice, and change the number of G-T I at the transmitter of Bob. The mismatch of the cascade G-T I number is shown in Fig. 7(a), it is known that the cascade G-T I number is a parameter that has a great influence on the group delay curve, the increase in the cascade number will change the amplitude of the group delay curve by multiples. Corresponding to 7(a), as long as the cascade numbers at both ends do not match, the system will show very poor synchronization.

The interferometer cavity length is a more sensitive parameter. When other parameters are matched, a G-T I is used in the transmitter of Alice and Bob, and the cavity length of G-T I at any end is changed. The relationship between the synchronization and mismatch of the cavity length is shown in Fig. 8, only 0.001% mismatch will lead to the CCF of the system below 0.9, which shows the sensitivity of the key. In addition, G-T I is a silicon-based optical device, and the accuracy of cavity length can reach a nanometer level. Here, the interferometer cavity length is centimeter level, so the adjustable cavity length space is  $10^6$ . The key space can be increased to  $10^{36}$  when six G-T Is are cascaded.

Then, comprehensively considering the influence of the above two parameters mismatch, six G-T Is are set at both ends, and the influence of the mismatch on the synchronization is studied when the cavity length mismatch is 0.01%, 0.1%, and 1%, respectively, shown in Fig. 9. It can be seen that the influence of the two parameters' mismatch on the system security is not a simple superposition. Since different parameter mismatches have different influences on the system, the superposition of multiple mismatches may cause an increase in the degree of synchronization. In practice, the most sensitive combination of interferometer parameters should be selected after simulation,

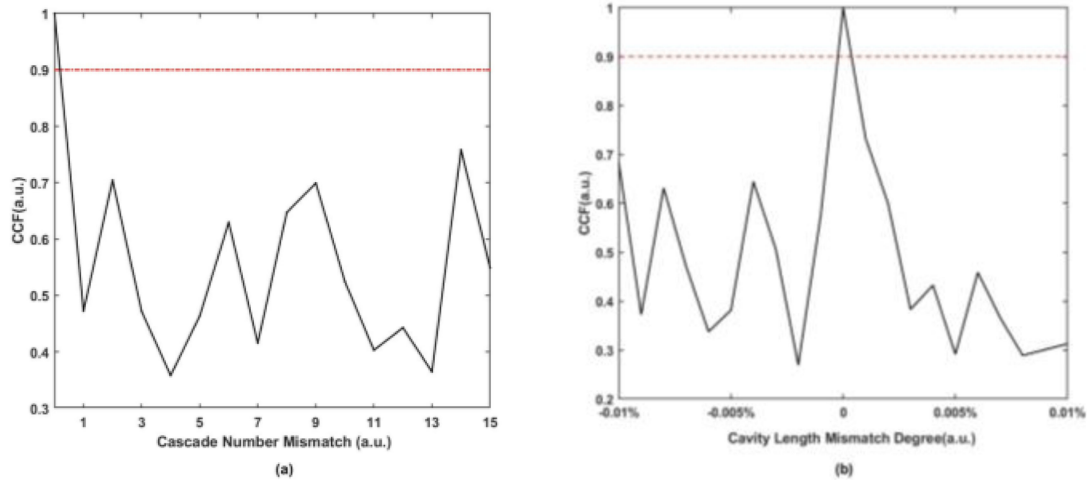


Fig. 7. (a) Relationship between G-T I number mismatch and system synchronization; (b) Relationship between G-T I cavity length mismatch and system synchronization.

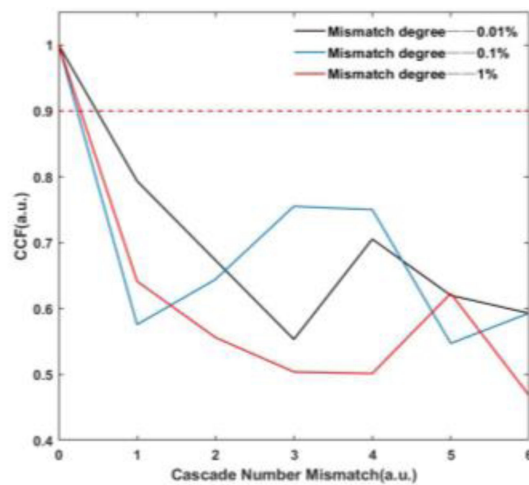


Fig. 8. Relationship between cascade number and cavity length mismatch and system synchronization.

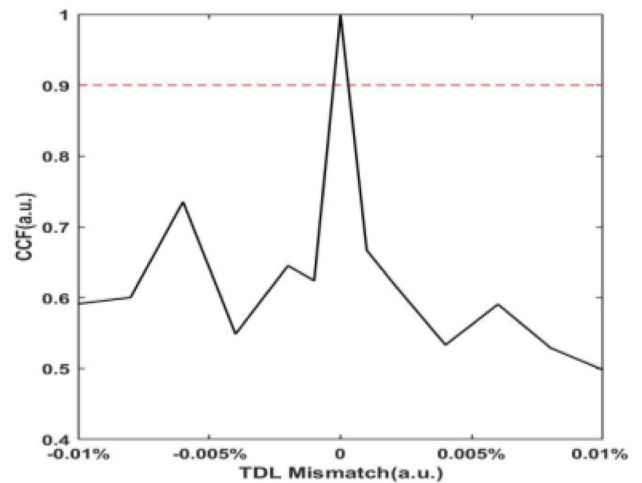


Fig. 9. TDL mismatch.

rather than blindly increasing cascade number and the complexity of cavity length.

The last dimensional key — the TDS of TDL, like the interferometer cavity length, can lead to a large key space for the system. Assuming that the other parameters are perfectly matched, we adjust only the TDS, when the mismatch rate is only 0.001%, the CCF value decreases to 0.7327. The reason is that the bandwidth nature of ASE noise makes the TDS a very sensitive key, which increases the security of the system.

## V. MESSAGE RECOVERY AND TRANSMISSION

Next, we use the proposed scheme to encrypt and decrypt messages. The schematic diagram of the multimode optical chaotic secure communication system is shown in Fig. 1. In Section II, we know that system can realize bidirectional and unidirectional interaction. The essence of these two interactions is the same. If the unidirectional transmission is to be carried out, it is only necessary to cancel the message at any end of the bidirectional transmission, and other operations remain

unchanged. To simplify the steps, the following operations are carried out under unidirectional transmission. Because the system can encrypt the intensity and phase of the messages at the same time, we try to encrypt and decrypt the 16QAM message and introduce the additive white Gaussian noise in the channel with SNR range [5,40]. The constellation diagram, eye diagram, and IQ waveform are shown in Fig. 10(a)–(c), respectively.

Then, we simulate the transmission of a binary message in optical fibers in OptiSystem, and dispersion compensation fibers (DCF) and amplifiers to compensate for dispersion and attenuation in optical fibers. DSP algorithm can also be used to compensate for the channel damage generated in the transmission process more accurately. [31], [32]. In the case of 1Gb/s, the relationship between distance and the BER is shown in Fig. 11(a), the forward error correction(FEC) technology can be used to recover the message, and the transmission distance can reach more than 70 km. In Fig. 11(c), the received message waveform trajectories under different distances are recorded. As the distance increases, the disturbance introduced becomes larger, leading to the increase of the BER.

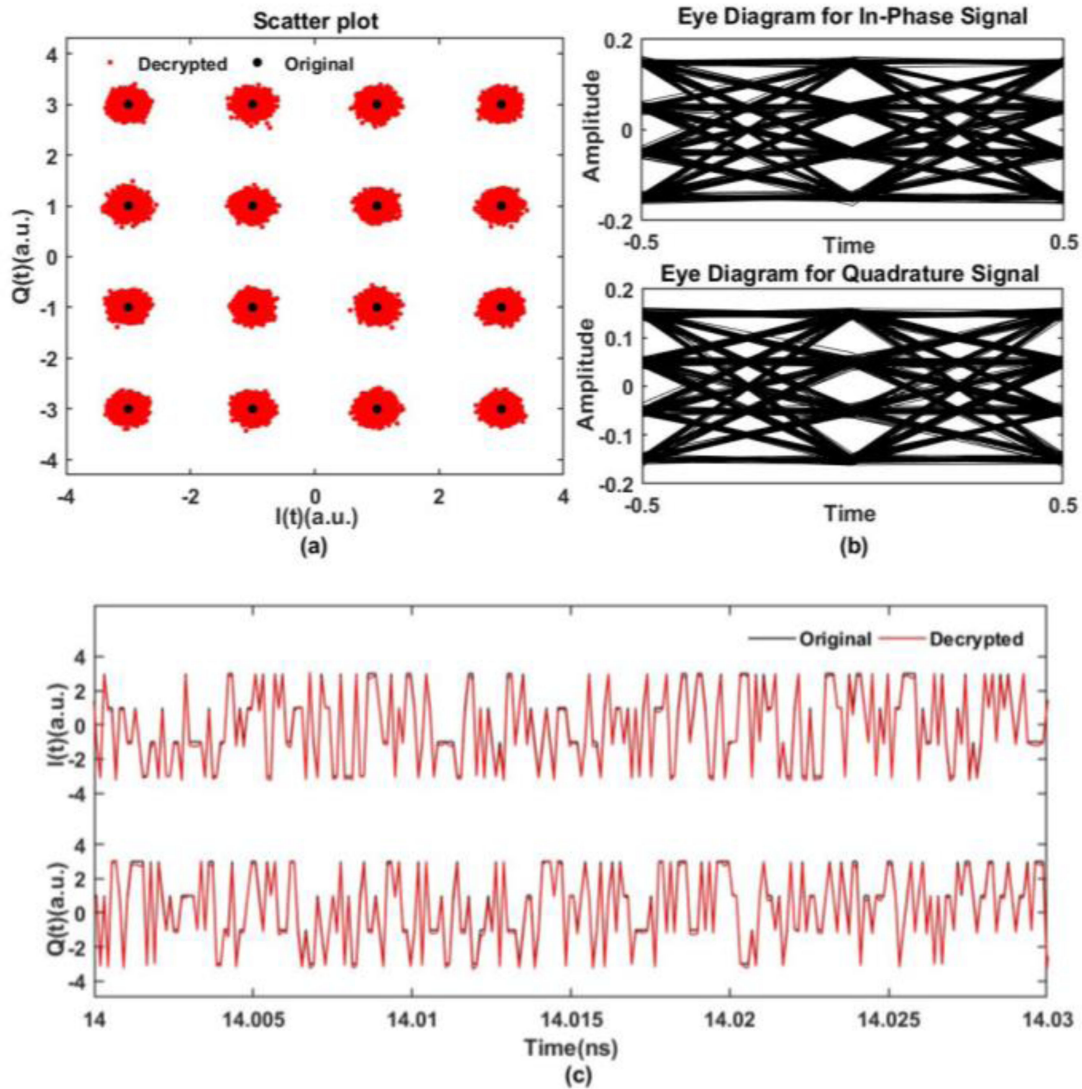


Fig. 10. (a) Constellation; (b) Eye diagram; (c) IQ waveform.

In daily life, the message rate in optical fiber communication is much larger than the 1Gb/s set in the above simulation process. To make the simulation more valuable, we continue to study the relationship between message rate and BER. By reserving the space for BER associated with the rate growth, we set the 10 km distance based on the data in Fig. 11(a), and the relationship between the message rate and the BER curve is shown in Fig. 12. When the message rate is 9 Gb/s, the corresponding BER below the FEC threshold. Therefore, the maximum message rate of 9 Gb/s can be achieved within a 10 km distance.

In Fig. 1, both Alice and Bob have two transmitters. In practical applications, the number of transmitters can be increased or reduced as required. However, the system has some shortcomings. Demand for equipment increases with the increase of channels [30], [33], which will introduce more optoelectronic devices and higher costs. In a harsh environment, the device's performance may be affected by environmental factors such as temperature and vibration. So it is better to use a general encryption device to encrypt different channels at the same time,

which can significantly save costs [34] and enhance the system stability, such as WDM security scheme [35], [36].

## VI. CONCLUSION

In conclusion, a multimode optical chaotic communication system with multidimensional keys and a complex entropy source is proposed. In this scheme, we use ASE noise as a complex entropy source to improve the security of the system and use G-TICG as an FDGD module to hide the TDS and disturb the chaotic sequences to increase the complexity of the system. The three-dimensional keys—cascade number, each G-T I cavity length, and TDS have strong sensitivity under the influence of ASE noise. Simulation results show that the system cannot effectively decrypt data only when the interferometer cavity length or TDS is in the mismatch of 0.001%, which proves that the system has strong security. The 16QAM signal and binary signal can be encrypted and decrypted. And when the binary message rate is 1Gb/s, the effective transmission of 75km can be achieved. When the transmission distance is 10km,



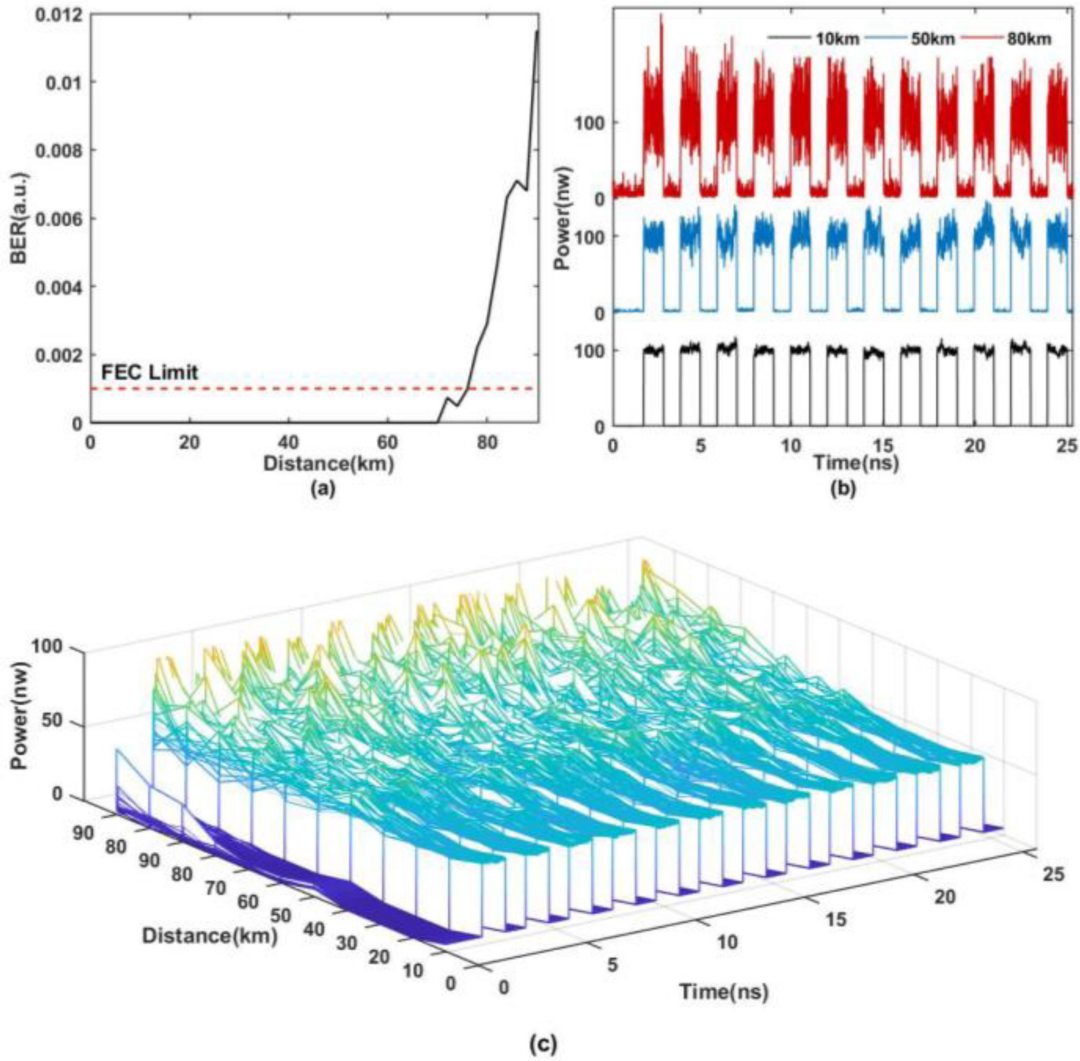


Fig. 11. (a) 1Gb/s, the relationship between distance and BER; (b) The received message waveform trajectories at 10 km, 50 km, and 80 km; (c) The received message waveform trajectories under different distances.

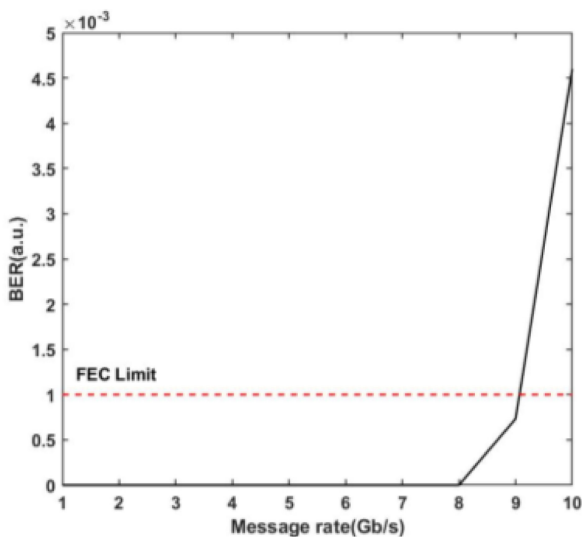


Fig. 12 10 km, the relationship between message rate and BER.

the maximum binary message rate can reach 9 Gb/s. Besides, combined with wavelength converter and wavelength division multiplexer, information interaction in multiple modes can be realized at the same time, the system improves the efficiency of transmission and realizes secure communication in various modes, which has wide application scenarios.

#### REFERENCES

- [1] G. Pérez and H. A. Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.*, vol. 74, no. 11, pp. 1970–1973, 1995.
- [2] D. Chen, Q. Li, and Q. Bao, "Bidirectional communication with time-delay concealment in a system combining all-optical intensity and electrooptical phase chaos," *Opt. Commun.*, vol. 465, 2020, Art. no. 124962.
- [3] V. S. Udaltsov et al., "Time delay identification in chaotic cryptosystems ruled by delay-differential equations," *J. Opt. Technol.*, vol. 72, no. 5, pp. 373–377, 2005.
- [4] 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. 879–1891, Jul. 2009.

- [5] L. Zunino, O. A. Rosso, and M. C. Soriano, "Characterizing the hyperchaotic dynamics of a semiconductor laser subject to optical feedback via permutation entropy," *IEEE J. Sel. Topics Quantum Electron.*, vol. 17, no. 5, pp. 1250–1257, Sep./Oct. 2011.
- [6] M. Cheng et al., "Time delay estimation from time series for optical chaos systems using deep Learning," *Opt. Exp.*, vol. 29, no. 5, pp. 7904–7915, 2021.
- [7] D. Rontani et al., "Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback," *Opt. Lett.*, vol. 32, no. 20, pp. 2960–2962, 2007.
- [8] R. M. Nguimdo et al., "Role of the phase in the identification of delay time in semiconductor lasers with optical feedback," *Opt. Lett.*, vol. 36, no. 22, pp. 4332–4334, 2011.
- [9] R. M. Nguimdo et al., "Loss of time-delay signature in chaotic semiconductor ring lasers," *Opt. Lett.*, vol. 37, no. 13, pp. 2541–2543, 2012.
- [10] R. Zhang et al., "Enhancing time-delay suppression in a semiconductor laser with chaotic optical injection via parameter mismatch," *Opt. Exp.*, vol. 28, no. 5, pp. 7197–7206, 2020.
- [11] S.-S. Li et al., "Chaotic time-delay signature suppression with bandwidth broadening by fiber propagation," *Opt. Lett.*, vol. 43, no. 19, pp. 4751–4754, 2018.
- [12] A. Zhao et al., "Parallel generation of low-correlation wideband complex chaotic signals using CW laser and external-cavity laser with self-phase-modulated injection," *Opto-Electron. Adv.*, vol. 5, no. 05, pp. 53–60, 2022.
- [13] D. Chang et al., "Flat broadband chaos generation in a discrete-mode laser subject to optical feedback," *Opt. Exp.*, vol. 28, no. 26, pp. 39076–39083, 2020.
- [14] R. M. Nguimdo et al., "Digital key for chaos communication performing time delay concealment," *Phys. Rev. Lett.*, vol. 107, no. 3, 2011, Art. no. 034103.
- [15] R. M. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," *Opt. Exp.*, vol. 20, no. 23, pp. 25333–25344, 2012.
- [16] T. T. Hou et al., "Maximizing the security of chaotic optical communications," *Opt. Exp.*, vol. 24, no. 20, pp. 23439–23449, 2016.
- [17] J. Hizanidis, S. Deligiannidis, A. Bogris, and D. Syvridis, "Enhancement of chaos encryption potential by combining all-optical and electro-optical chaos generators," *IEEE J. Quantum Electron.*, vol. 46, no. 11, pp. 1642–1649, Nov. 2010.
- [18] G. Aromataris and V. Annovazzi-Lodi, "Enhancing privacy of chaotic communications by double masking," *IEEE J. Quantum Electron.*, vol. 49, no. 11, pp. 955–959, Nov. 2013.
- [19] G. D. Van Wiggeren and R. Roy, "Communication with chaotic lasers," *Science*, vol. 279, no. 5354, pp. 1198–1200, 1998.
- [20] B. Wu et al., "Optical steganography based on amplified spontaneous emission noise," *Opt. Exp.*, vol. 21, no. 2, pp. 2065–2071, 2013.
- [21] B. Wu et al., "Temporal phase mask encrypted optical steganography carried by amplified spontaneous emission noise," *Opt. Exp.*, vol. 22, no. 1, pp. 954–961, 2014.
- [22] Y. D. 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, 2019.
- [23] L. Li et al., "Design of a dual-cavity Gires-Tournois interferometer for multi-channel chromatic dispersion," *J. Optoelectron. Laser*, vol. 13, no. 8, pp. 802–805, 2002.
- [24] N. Jiang et al., "Generation of flat wideband chaos with suppressed time delay signature by using optical time lens," *Opt. Exp.*, vol. 25, no. 13, pp. 14359–14367, 2017.
- [25] K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Opt. Commun.*, vol. 30, no. 2, pp. 257–261, 1979.
- [26] R. M. Nguimdo, P. Colet, and C. Mirasso, "Electro-optic delay devices with double feedback," *IEEE J. Quantum Electron.*, vol. 46, no. 10, pp. 1436–1443, Oct. 2010.
- [27] L. L. Yi and J. X. Ke, "Research progress of chaotic secure optical communication," *J. Commun.*, vol. 41, no. 3, pp. 168–181, 2020.
- [28] L. Zhang, B. Liu, X. Xin, Q. Zhang, J. Yu, and Y. Wang, "Theory and performance analyses in secure CO-OFDM transmission system based on two-dimensional permutation," *J. Lightw. Technol.*, vol. 31, no. 1, pp. 74–80, Jan. 2013.
- [29] X. Gao et al., "Robust chaotic-shift-keying scheme based on electro-optical hybrid feedback system," *Opt. Exp.*, vol. 28, no. 8, pp. 10847–10858, 2020.
- [30] L. S. Wang et al., "Scheme of coherent optical chaos communication," *Opt. Lett.*, vol. 45, no. 17, pp. 4762–4765, 2020.
- [31] Y. Fu et al., "Analog-digital hybrid chaos-based long-haul coherent optical secure communication," *Opt. Lett.*, vol. 46, no. 7, pp. 1506–1509, 2021.
- [32] Y. Wu et al., "Capacity expansion of chaotic secure transmission system based on coherent optical detection and space division multiplexing over multi-core fiber," *Opt. Lett.*, vol. 47, no. 3, pp. 726–729, 2022.
- [33] Q. C. Zhao and H. X. Yin, "Performance analysis of dense wavelength division multiplexing secure communications with multiple chaotic optical channels," *Opt. Commun.*, vol. 285, no. 5, pp. 693–698, 2012.
- [34] Z. Gao et al., "40Gb/s secure optical communication based on symbol-by-symbol optical phase encryption," *IEEE Photon. Technol. Lett.*, vol. 32, no. 14, pp. 851–854, Jul. 2020.
- [35] N. Jiang et al., "Secure WDM-PON based on chaos synchronization and subcarrier modulation multiplexing," *J. Opt. Soc. Amer. B*, vol. 33, no. 4, pp. 637–642, 2016.
- [36] N. Jiang et al., "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, pp. 1536–1539, 2019.