photonics

MDPI

Communication

Analog–Digital Combined High-Secure Optical Communication System Based on Chaotic Circuit Driving

Qing Zhong [1,2,3], Bo Liu [1,2,3,*], Jianxin Ren [1,2,3], Yicheng Jiang [4], Rahat Ullah [1,2,3], Zhiruo Guo [1,2,3], Yaya Mao [1,2,3], Xiangyu Wu [1,2,3], Yongfeng Wu [1,2,3], Lilong Zhao [1,2,3] and Tingting Sun [1,2,3]

[1] Institute of Optics and Electronics, Nanjing University of Information Science & Technology, Nanjing 210044, China
[2] Jiangsu Key Laboratory for Optoelectronic Detection of Atmosphere and Ocean, Nanjing University of Information Science & Technology, Nanjing 210044, China
[3] Jiangsu International Joint Laboratory on Meterological Photonics and Optoelectronic Detection, Nanjing University of Information Science & Technology, Nanjing 210044, China
[4] School of Physics and Optoelectronic Engineering, Nanjing University of Information Science & Technology, Nanjing 210044, China
* Correspondence: bo@nuist.edu.cn

Abstract: We propose and demonstrate a new analog–digital combined high-secure optical communication system based on chaotic circuit driving, which achieves encryption in the analog and digital domains. A 3D chaotic system is used for analog domain phase encryption (ADPE) and digital domain time–frequency encryption (DDTFE) simultaneously. The ADPE is carried out by the privately chaotic signal driving the phase modulator (PM), which realizes chaotic phase encryption. The chaotic circuit comprehends highly complex nonlinear dynamics. Its size is 10 cm × 5 cm, which has the characteristics of small size and low cost. The DDTFE is performed by the frequency–time encryption of signals in the digital domain. The experimental results show that the optical physical layer encryption scheme based on analog and digital combination can successfully mask the original data. The driving signal of PM is that generated by the chaotic circuit and needs to be privately synchronized, so that the legal receiver may accurately decrypt the encrypted data and the eavesdropper is unable to intercept a valuable message. If the chaotic driving circuit produces a delay of 3 s, the bit error rate (BER) reaches more than 0.3 at the receiver. The results of experiment verify that the scheme can transmit 13.3 Gb/s 16 quadrature amplitude modulation orthogonal frequency division multiplexing (16QAM-OFDM) signal over 25 km standard single mode fiber (SSMF). This scheme achieves low-cost, high-security communication, making it a suitable foundation for high-speed, secure optical communication at the physical layer.

Keywords: high security; optical communication; chaotic encryption

Citation: Zhong, Q.; Liu, B.; Ren, J.; Jiang, Y.; Ullah, R.; Guo, Z.; Mao, Y.; Wu, X.; Wu, Y.; Zhao, L.; et al. Analog–Digital Combined High-Secure Optical Communication System Based on Chaotic Circuit Driving. *Photonics* **2022**, *9*, 669. https://doi.org/10.3390/photonics9090669

Received: 10 August 2022
Accepted: 12 September 2022
Published: 19 September 2022

1. Introduction

With the rapid development of digitization and computing power in information society, communication security is facing imminent threat. The majority of previously announced security enhancement strategies use algorithmic encryption, most commonly the advanced encryption standard (AES) [1–4], while algorithm-level encryption may be intercepted and cracked as a result of the advent of quantum computing [5]. The chaotic system has the characteristics of broad bandwidth, good randomness and high sensitivity [6–10]. At present, chaotic secure optical communication at the physical layer has become an effective strategy to protect the security of large-scale data exchange in modern networks [11].

Chaotic signals are generated by analog and digital methods. The former can generate highly complex nonlinear dynamic broadband signals [12]. In the field of optical communication, most chaotic signals in the analog domain are generated by chaotic lasers,

which are large in volume, high in cost and complex in structure. At the same time, these schemes pose higher requirements on chaotic synchronization, which is very important for a secure communication system based on a chaotic system [13]. The latter will pay for computational time when obtaining a more complex nonlinear dynamic behavior [14–16]. When the chaotic signal is used as the carrier for chaotic secure communication, its spectral efficiency is low, and when the transmission rate is low, the information is easy to be intercepted [17]. On the other hand, some scholars also adopt chaotic signal to drive phase modulator (PM) and scramble private chaotic phase [18]. The process should convert the complicated nonlinear electro-optical signal and be injected into PM, which makes the optical layer encryption possibly. It can also encrypt the whole network data of low delay and high speed [19]. However, the chaotic laser produces complexly and carries out nonlinear electro-optical signal converting. The variety of optical damage will inevitably cause signal distortion [20]. It also significantly increases the cost, and the application of the scheme is impeded by these problems.

In this paper, we propose an analog–digital combined high-secure optical communication system. The scheme adopts a 3D chaotic system, and x is the injected signal of the PM to carry out phase disturbance in the analog domain. With a chaotic circuit instead of chaotic laser as a driving signal to be injected into the PM, the complicated nonlinear electro-optical signal conversion problem of existing schemes is solved. This scheme reduces the cost and optimizes the size. The y and z are used for the time–frequency domain encryption in the digital domain. Moreover, we demonstrate a 13.3 Gb/s encrypted signal transmission over 25 km standard single-mode fiber (SSMF). If the chaotic driving circuit produces a delay of 3 s, the bit error rate (BER) reaches more than 0.3 at the receiver. The results show that the analog–digital combined encrypted scheme based on the chaotic circuit as driving signal has a good performance in optical communication system and is compatible with the existing optical networks.

2. Principles

In Figure 1, we present the schematic diagram of the proposed analog–digital combined high-secure optical communication system. The encryption module is made up of two encrypting portions: digital and analog. The unified 3D chaotic system generates chaotic signals for the analog-digital combined encryption. In the analog part, x chaotic signal is generated by the corresponding circuit of the chaotic system to encrypt the phase. In the digital part, the y and z sequences of the chaotic system are generated by MATLAB to encrypt the data in the time and frequency domain. At the receiver, the PM is demodulated by using chaotic circuit to generate chaotic signal, which is opposite to the x chaotic signal. Then, the digital signal processing (DSP) performs the opposite operation with the transmitter to decrypt in the digital domain.

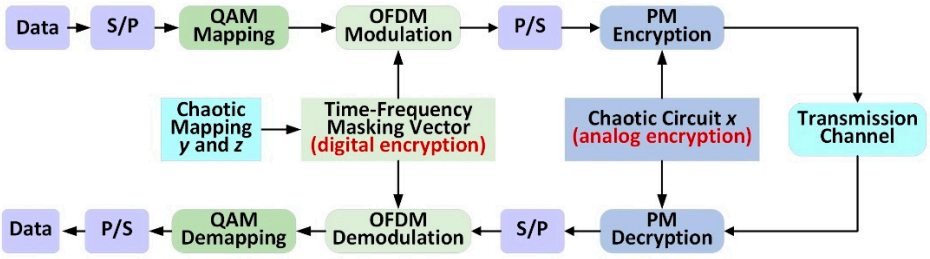

Figure 1. Schematic diagram of the proposed encryption scheme.

Employing the following 3D chaotic system to generate a chaotic signal to encrypt the original data:

$$\begin{cases} \dot{x} = y \\ \dot{y} = z \\ \dot{z} = -az + b\mathrm{sgn}(x) - x - y \end{cases} \quad (1)$$

when $a = 0.6$, $b = 1$, and $(x_1, y_1, z_1) = (0, 0, 1)$, the system (1) is in a chaotic orbit, as shown in Figure 2.

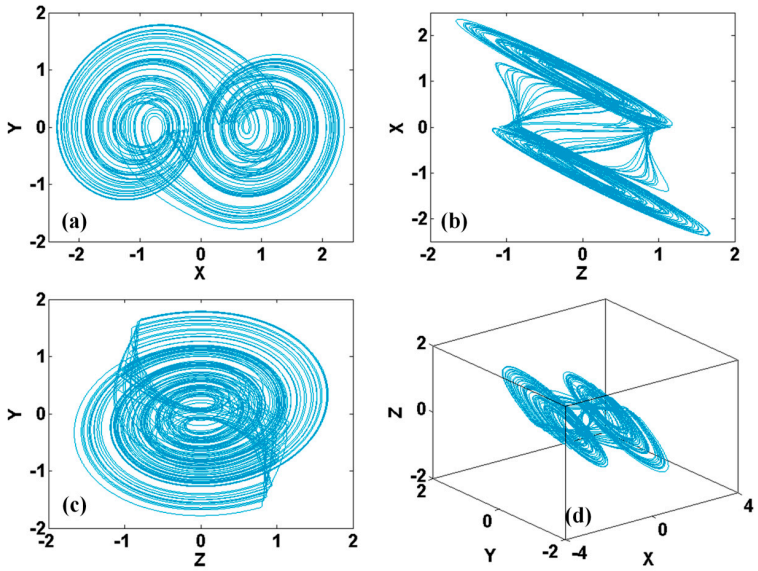

Figure 2. Phase trajectory diagram of the chaotic system. (**a**) the phase trajectory of x–y, (**b**) the phase trajectory of z–x, (**c**) the phase trajectory of z–y, and (**d**) the phase trajectory of x–y–z.

We designed the chaotic circuit corresponding to the chaotic system to implement the encryption on the hardware. The proposed scheme utilizes the chaotic signal generated by the chaotic circuit to drive the PM to encrypt rather than the optical carrier, and the transmission capacity is no longer limited by the bandwidth of the chaotic signal. The chaotic circuit has the characteristics of small size, low cost and high sensitivity. Its size is only 10 cm × 5 cm. The circuit is composed of three channels, which are integrated according to the state variables x, y, and z, respectively. The circuit schematic of system (1) was designed as shown in Figure 3. The construction of the corresponding chaotic circuit can be represented as:

$$\begin{cases} \dot{x} = \frac{1}{R_1 C_1} y \\ \dot{y} = \frac{1}{R_2 C_2} z \\ \dot{z} = -\frac{1}{R_7 C_3} z + \frac{1}{R_8 C_3} \mathrm{sgn}(x) - \frac{1}{R_5 C_3} x - \frac{1}{R_6 C_3} y \end{cases} \tag{2}$$

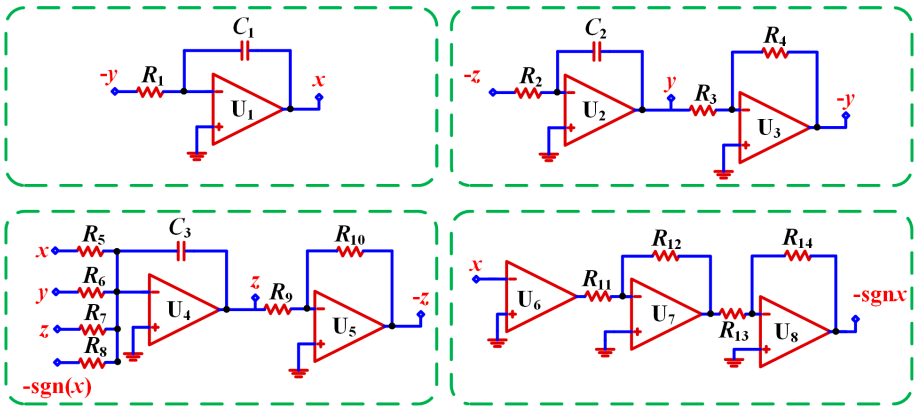

Figure 3. Chaotic circuit schematic diagram.

The chaotic circuit completes the computing of integral, addition, subtraction and nonlinear operations. The supply voltage of the circuit is ±13.5 V. The corresponding circuit components can be selected as:

$$\begin{cases} C_1 = C_2 = C_3 = 100\ \text{nF},\ R_1 = 16.6\ \text{K}\Omega \\ R_2 = R_3 = R_4 = R_5 = R_6 = R_7 = R_8 = R_9 = R_{10} = R_{13} = R_{14} = 10\ \text{K}\Omega \\ R_{11} = 13.5\ \text{K}\Omega,\ R_{12} = 1\ \text{K}\Omega \end{cases} \quad (3)$$

The type specification of operational amplifier is LM741CN. The physical equipment of the analog circuit is shown in Figure 4a. The phase trajectory of the analog circuit in the oscilloscope shows in Figure 4b,c. Figure 4b is the phase trajectory of x–y, and Figure 4c is the phase trajectory of y–z. The outputs waveform of the physical circuit is consistent with the simulation outputs. The temporal waveform of the generated chaotic signal x is shown in Figure 4d. Figure 4e shows the spectrum of the generated chaotic signal x. The results indicate the typical characteristics of chaotic signal, including random like-noise in the time domain and the wide bandwidth in the frequency domain. There are the Lyapunov exponent of the signal greater than 0, which exhibits the chaotic properties of the x signal. The autocorrelation function (ACF) can prove the high randomness. Figure 4f shows the autocorrelation of the x chaotic signal. As can be seen from the results in Figure 4f, there are no similar fragments in the x chaotic signal. In this scheme, the x signal generated by the chaotic circuit is used to encrypt the data, and the x chaotic signal is injected into PM as the driving signal to disturb the phase. The amplitude of the driving signal of PM 1 is opposite to that of the driving signal of PM 2. The chaotic circuits at the transmitter and receiver are controlled by the same power supply, which ensures the synchronization of chaotic signals.

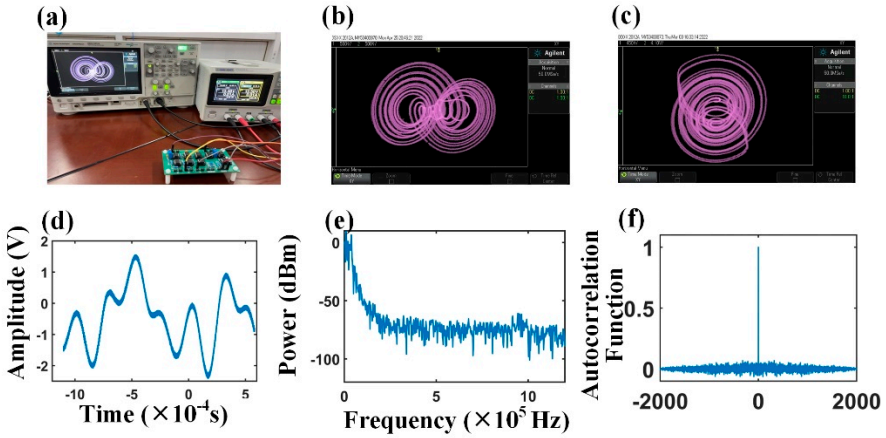

Figure 4. (**a**) Physical equipment of the analog circuit, (**b**) x–y phase trajectory, (**c**) y–z phase trajectory, (**d**) temporal waveform, (**e**) spectrum, and (**f**) autocorrelation.

When the chaotic signal is injected into the PM, the adapter needs to be connected, which has a 50 Ohms impedance. This affects the chaotic waveform and the nonlinear dynamic characteristics of chaos disappear. Therefore, in this scheme, the chaotic circuit module needs to be connected in series with the amplifying matching module to realize the matching between modules, and the amplification of the chaotic signal is conducive to signal encryption. The specific flow chart is shown in Figure 5. The voltage is adjusted according to the feedback signal of the common emitter amplifier circuit.

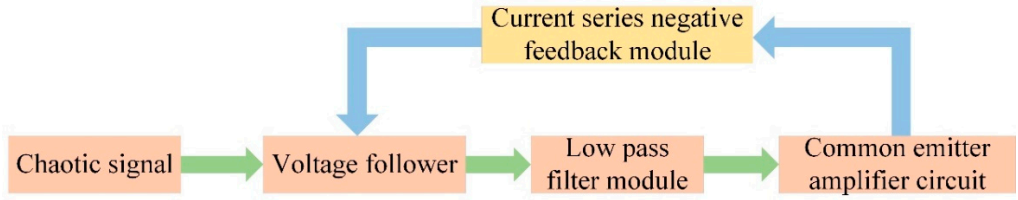

Figure 5. Amplifying matching circuit flow chart.

The main function of this module is realized by a triode. Due to the randomness and non-periodicity of chaotic signals, it is more challenging to amplify and match chaotic signals. If the chaotic signal is directly connected to the triode, waveform distortion or signal self-excitation may occur. Therefore, it is necessary to add a voltage follower module, low-pass filter module and current series negative feedback module to match and adjust. The specific circuit schematic diagram is shown in Figure 6.

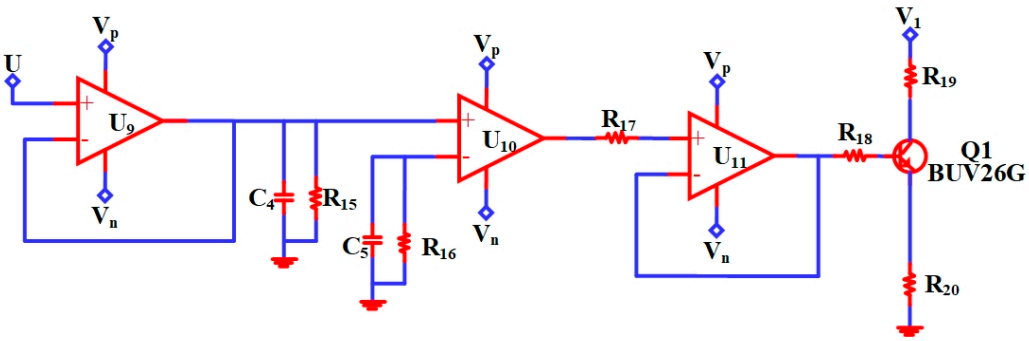

Figure 6. Amplifying matching circuit schematic diagram.

In Figure 6, the amplification matching circuit is mainly composed of resistance–capacitance parallel R_{15} and C_4, R_{16} and C_5, operational amplifiers U_9 and U_{10}, current-limiting resistance R_2 and R_{13}, triode Q1BUV26G, current feedback sampling resistance R_{18}, load resistance R_{19} and Vp power supply. The adapted voltage follower, which is made up of the operational amplifier U_9, is designed to match the chaotic signal source of the output to that of the input and perform impedance matching, allowing the signal of the amplifier circuit to operate within its normal range. At the same time, it has an isolation effect and can cut off the interference effect of the back electromotive force on the front stage. The low frequency signal can thus flow normally through the low pass filter module, which is made up of inductance and capacitance. The output signal is injected into the voltage follower composed of operational amplifiers U_9 and U_{10}, where resistors R_{17} and R_{18} are used for limiting the current. Finally, the signal is injected from the base of the triode, and the emitter outputs the amplified chaotic signal. Since the signal is input from the base and output from the emitter, the common emitter amplifier circuit is formed. The signal is transmitted back to a low-pass filter module made up of an inductor and capacitor through a feedback loop. The corresponding circuit components can be selected as:

$$\begin{cases} C_4 = C_5 = 22\ \text{nF},\ R_{15} = R_{16} = 1000\ \text{K}\Omega \\ R_{17} = R_{18} = 100\ \text{K}\Omega,\ R_{19} = 3\ \Omega,\ R_{20} = 2\ \Omega \end{cases} \tag{4}$$

The purpose of this design is to increase load capacity and stabilize output voltage.

The physical equipment of the amplification matching circuit is shown in Figure 7a. The temporal waveform after the amplification matching circuit is shown in Figure 7b. The maximum output signal value is about 6.5 V. The cross-correlation (CC) function between chaotic circuit 1 and chaotic circuit 2 is shown in Figure 7c. It is indicated that outputs of

chaotic circuit 1 and chaotic circuit 2 are well synchronized with the CC of 0.99. The CC can be expressed as:

$$CC = \frac{\sum_{i=0}^{n-1}[(x_i - \mu_x)(y_i - \mu_y)]}{\sqrt{\sum_{i=0}^{n-1}(x_i - \mu_x)^2 \cdot \sum_{i=0}^{n-1}(y_i - \mu_y)^2}} \quad (5)$$

where μ_x and μ_y denote the mean of the time series of the chaotic circuit 1 and the chaotic circuit 2, respectively.

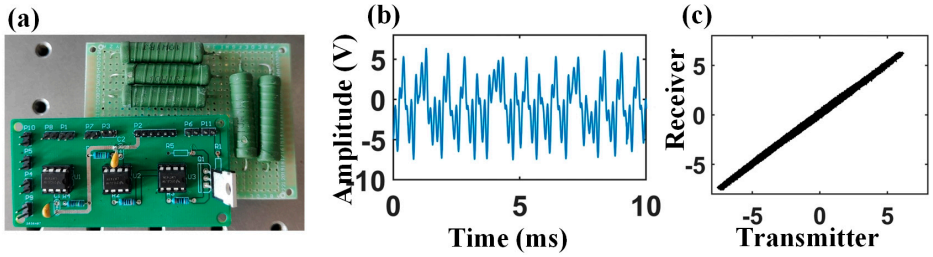

Figure 7. (**a**) Physical equipment of the amplifying matching circuit, (**b**) temporal waveform after amplifying, and (**c**) cross-correlation between chaotic circuit 1 and chaotic circuit 2.

A schematic of digital domain encryption is shown in Figure 8. The 16 quadrature amplitude modulation orthogonal frequency division multiplexing (16QAM-OFDM) modulation was adopted in our scheme. In order to reduce the complexity of the algorithm and improve the bit error performance, we designed an optimization algorithm. Firstly, as shown in Figure 8a, the sub-bands in the frequency domain are divided. As is shown in Figure 8b, the sub-bands in the frequency domain are disturbed, in order to reduce the number of disturbed objects in the frequency domain. Then, the encryption in the time domain is shown in Figure 8c. The optimization scheme of region division is not used in the time domain, so as to achieve the effect of all information scrambling. It was assumed that the process of OFDM has M subcarriers for data transmission. It can be divided into K frequency bands according to region division, and each frequency band has n sub-bands. Its relation satisfies $M = K \times n$. The number of frequency bands K can be selected, but K must be greater than 3. A total of 512 subcarriers were used for data transmission, and the four subcarriers were divided into a frequency band, with a total of 128 frequency bands. Frequency domain encryption is to perturb the 128 frequency bands. Compared with the undivided frequency band algorithm, the computational cost of the proposed algorithm was reduced by four times, and all the data were perturbed and encrypted.

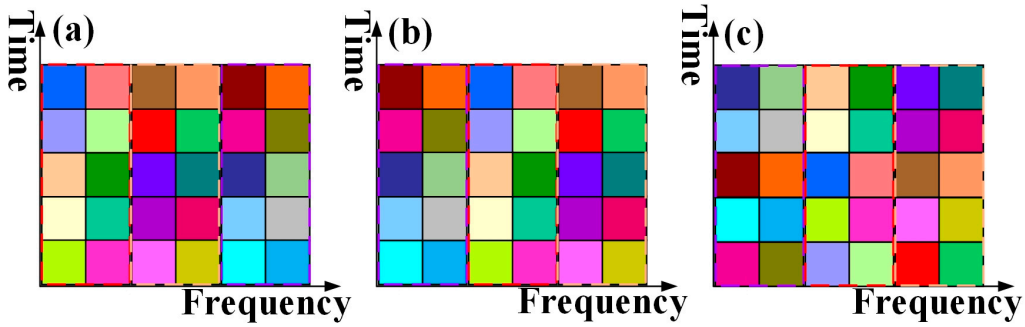

Figure 8. Schematic of the proposed digital domain encryption. (**a**) the divided frequency domain, (**b**) the disturbed frequency domain, and (**c**) the disturbed time domain.

The chaotic sequence $\boldsymbol{y}$ was used in this encryption part, but the original chaotic sequence did not meet the requirements of signal encryption, so it needed to be optimized, as shown in the following process:

$$\boldsymbol{Y} = Mat\left\{ mod(\boldsymbol{y}\cdot 10^2, 1)\cdot[mod(\boldsymbol{y}\cdot 10^2, 1)']\right\} \tag{6}$$

where $Mat\{\cdot\}$ means to set the non-integer element of the matrix to 0, and $\boldsymbol{Y}$ is the generated permutation matrix. The encrypted information in frequency domain can be expressed as:

$$\begin{bmatrix} F_{e1} \\ F_{e2} \\ \vdots \\ F_{ek} \end{bmatrix} = \begin{bmatrix} F_1 \\ F_2 \\ \vdots \\ F_k \end{bmatrix} \cdot \boldsymbol{Y} \tag{7}$$

where F_{ek} is the signal of encrypted frequency band and F_k is the signal of original frequency band.

The data of the time domain are perturbed so that all data are encrypted. The data are interleaving diffusion perturbation by the optimized chaotic sequence. Zoning perturbation was not used; otherwise, the data are only scrambled in a local area, which increases the possibility of cracking. The specific processing of chaotic sequence can be expressed as:

$$\boldsymbol{Z} = Mat\left\{ mod(\boldsymbol{z}\cdot 10^2, 1)\cdot[mod(\boldsymbol{z}\cdot 10^2, 1)']\right\} \tag{8}$$

To improve the encryption performance and enhance the robustness of the system against proportional cracking, encrypted data in the time domain can be expressed as:

$$T_e = T\cdot\boldsymbol{Z} \tag{9}$$

where T is the original time domain data and T_e is the encrypted time domain data. At the receiver, the encryption algorithm is reversible, and the data can be decrypted by the reverse operation of the encryption process.

3. Experiment Setup and Results

The device diagram of the experimental equipment is shown in Figure 9, and the intensity modulation direct detection (IM/DD) system based on 25 km SSMF is established. The attenuation of the SSMF is less than 0.2 dB/km, the dispersion is less than 18 ps/(nm·km), the effective group refractive index is 1.467, and the cladding diameter is 125.0 ± 0.7 μm. In addition, DSP technology and phase modulator were used to encrypt digital domain and analog domain, respectively. The encrypted signal at the digital end was loaded into arbitrary waveform generator (AWG, TekAWG70002A) with a sampling rate of 15 GSa/s. The analog signal after amplification by an electrical amplifier (EA) was injected into Mach–Zehnder modulator (MZM) to realize photoelectric modulation. The wavelengths and power of the laser were set at 1550 nm and 10 dBm, respectively. The output signal of the MZM was sent to PM 1 for phase encryption perturbation. The half-wave voltage of the PM was 6 V. The modulation depth was equal to 2. The modulation depth is defined as the ratio of the peak-to-peak value of the modulated wave to the half-wave voltage of the PM. The drive signal of PM 1 was generated by the chaotic circuit. After being amplified by an erbium-doped fiber amplifier (EDFA), the modulated optical signal was launched into 25 km SSMF. It is worth mentioning that the radio frequency (RF) signals of the intensity modulator and the phase modulator are independent, so there is no correlation between the rates of the intensity modulator and the phase modulator. The RF signal out by AWG was modulated to the light by the intensity modulator, and the optical carrier carrying the information was modulated by the independent phase modulator for perturbation. The modulation depth has a great influence on the encryption effect. The modulation depth

of the proposed scheme reached 2, which can complete the encryption of information. At the receiver, the chaotic circuit 2 was used to drive PM 2 for decryption, and we adjusted the received optical power by a variable optical attenuator (VOA). A photodiode (PD) was used for signal detection. A mixed signal oscilloscope (MSO, TekMSO73304DX) with a sampling rate of 50 GSa/s was used for analog-to-digital conversion (ADC). DSP technology was used to decrypt signal in the digital domain. The total bit rate of the OFDM signal can be tantamount to the expression of (subcarrier number × entropy × AWG sampling rate/IFFT size/(1 + CP)). CP is the length of the cyclic prefix to avoid data crosstalk. In this scheme, the length of CP was 1/8 of the data, and the number of IFFT points was 2048. This modulation scheme was 4 bit/symbol, and subcarrier number was 512. So, the scheme can transmit 13.3 Gb/s 16QAM-OFDM signal. The devices on the transmitter had AWG, Laser, MZM, EA, PM 1, EDFA, and chaotic circuit 1. The devices on the receiver had PM 2, VOA, PD, and MOS. The control power was used to control chaotic circuits.

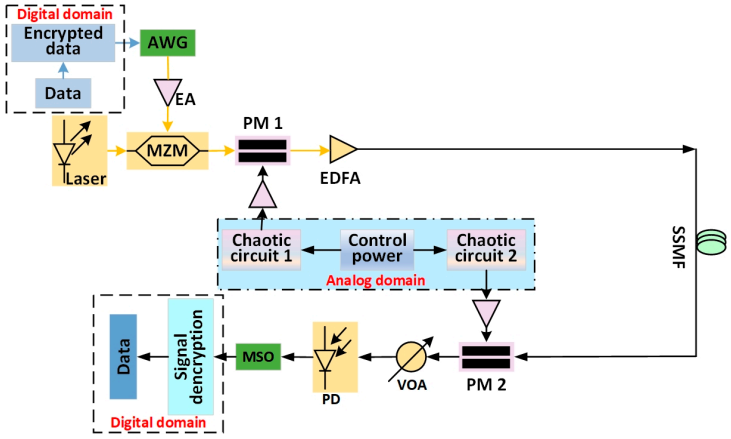

Figure 9. Experimental setup (AWG: arbitrary waveform generator; MZM: Mach–Zehnder modulator; EDFA: erbium-doped fiber amplifier; PM: phase modulator; VOA: variable optical attenuator; PD: photodiode; MSO: mixed signal oscilloscope).

Figure 10 shows the BER curve of the synchronous 16QAM-OFDM signal and the signal of a 3 s delay decryption under different receiver power after 25 km SSMF. As can be seen from Figure 10, when the receiver and transmitter can synchronize, the signal can be decrypted normally. As the received optical power decreases, the BER of the signal increases. When there is a 3 s delay between the chaotic circuit 2 and chaotic circuit 1, the signal cannot be decrypted normally, and the BER reaches more than 0.3. It is worth mentioning that, when the delay is set to more than 3 s, the information on the receiver cannot be recovered normally. If the chaotic circuit with higher bandwidth is adopted, the synchronization requirement of chaotic circuit 1 and 2 will be stricter. The data after PM 1 are directly recovered, and the decryption of PM 2 and digital end is no longer carried out. The BER after PM 1 is above very high, as can be seen from the experimental results. The results show that the transmitted data have reached the effect of scrambling and masking under the encryption of the digital domain and analog domain. In addition, we also used the incorrect keys to decrypt it, and the results show that the data are difficult to recover.

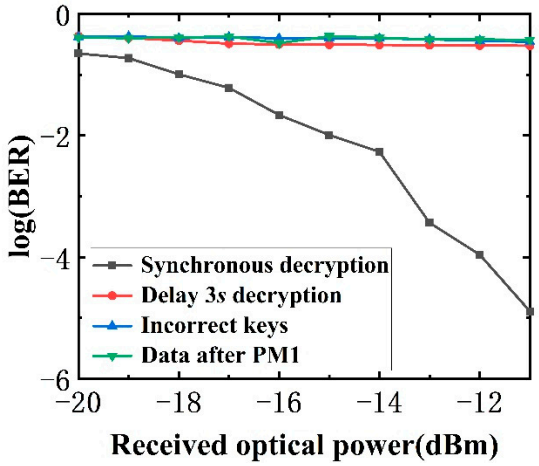

Figure 10. BER performance under different receiver power values.

In addition, we also tested the constellation points in different scenarios, as shown in Figure 11, respectively showing the original constellation diagram (a), the encrypted data constellation diagram (b), the restored constellation diagram after 25 km optical fiber transmission (c), and the restored constellation diagram after back-to-back (BTB) (d). It is also clear from the constellation diagram that this scheme can recover the information well. In the case of the unknown key and encryption mechanism, the data are difficult to recover, and its constellation is a mess, as shown in Figure 11b.

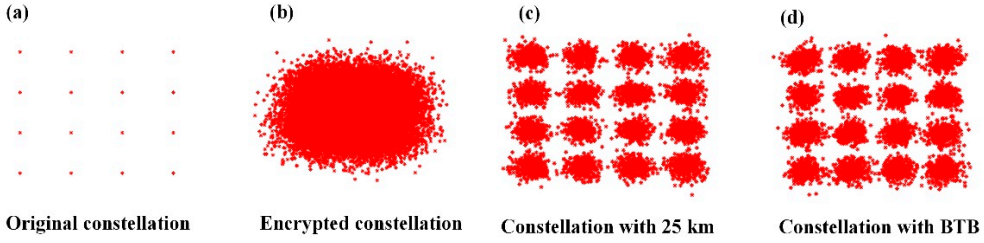

Figure 11. Constellation diagram for different scenarios. (**a**) the original constellation diagram, (**b**) the encrypted data constellation diagram, (**c**) the restored constellation diagram after 25 km optical fiber transmission, and (**d**) the restored constellation diagram after BTB.

In order to verify the security of the proposed scheme, we also carried out the sensitivity test of the proposed scheme and whether the data can be recovered normally when the key is perturbed. In the concrete implementation scheme, we used the perturbed key to decrypt the transmitted data. It can be seen from Figure 12 that, when the perturbation degree of x, y and z reaches E-6, there is a large bit error in the data and the data cannot be recovered normally. The coordinate of curve x at E-6 represents the BER after decrypting the information when the value 0 of the parameter x in the key is changed to $0 + 10^{-6}$. When the perturbation degree of the control parameter a and b reaches E-8, the data cannot be recovered normally. The experimental results show that the information can be recovered correctly only when the receiver obtains the correct key. For the eavesdropper, when the value difference between the cracked key and the correct key reaches E-8, the data are difficult to recover. The scheme ensures the security of data transmission.

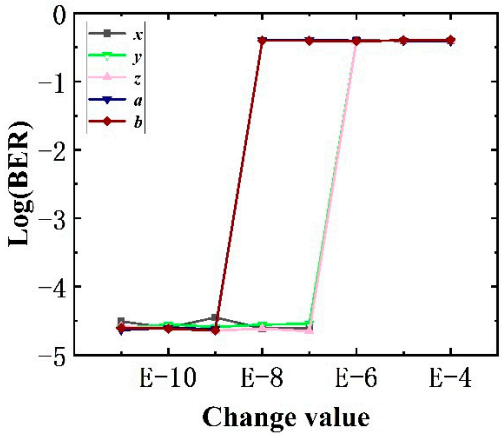

Figure 12. The curves of BER with a tiny change in the initial value.

4. Discussion

The proposed scheme performs double encryption in the digital domain and analog domain, taking into account the advantages of both encryption methods. The scheme can effectively protect data transmission. Data can be recovered accurately at the receiver. When the received optical power is above −10 dBm, BER can reach 0. The encryption method of the digital domain shows the advantage of more flexibility and can guarantee the encrypted effect. The encryption of the analog domain can reflect the more complex nonlinear dynamics of the chaotic system. The digital encryption method is derived from chaotic system mapping by computers, which requires the precision of a computer. If the equipment is not precise enough, the output sequence no longer has strict chaotic dynamics. Therefore, the enhanced dynamic characteristics of chaotic systems in optical physical layer encryption will be studied in the following research.

5. Conclusions

In conclusion, the new analog–digital combined high-secure physical layer encryption optical communication system was proposed to protect data transmission. The chaotic signal generated by the chaotic circuit can encrypt the data as the driving signal. Compared with the traditional chaotic light source, this scheme avoids the nonlinear conversion of photoelectric signal. In the process of combining the digital domain and the analog domain, it can effectively double encrypt data and has a promising secure transmission scheme for future applications.

Author Contributions: Conceptualization, Q.Z. and B.L.; methodology, Q.Z., J.R. and Z.G.; formal analysis, Q.Z., J.R., Y.M. and Y.J.; data curation, Q.Z. and Y.J.; writing—original draft preparation, Q.Z. and Z.G.; writing—review and editing, Q.Z., R.U., X.W., Y.W., L.Z. and T.S.; funding acquisition, B.L., Y.W., L.Z. and T.S. All authors have read and agreed to the published version of the manuscript.

Funding: National Key Research and Development Program of China (No. 2018YFB1801703); National Natural Science Foundation of China (No. 61875248, 61835005, 62171227, 61727817, U2001601, 62035018, 61935005, 61935011, 61720106015, and 61975084); Jiangsu team of innovation and entrepreneurship; The Startup Foundation for Introducing Talent of NUIST.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jing, N.; Zhao, A.; Xue, C.; Tang, J.; Qiu, K. Physical secure optical communication based on private chaotic spectral phase encryption/decryption. *Opt. Lett.* **2019**, *44*, 1536–1539. [CrossRef] [PubMed]
2. Zhang, L.; Liu, B.; Xin, X. Secure optical generalized filter bank multi-carrier system based on cubic constellation masked method. *Opt. Lett.* **2015**, *40*, 2711–2714. [CrossRef] [PubMed]

3. Buchmann, J.; Braun, J.; Demirel, D.; Geihs, M. Quantum cryptography: A view from classical cryptography. *Quantum Sci. Technol.* **2017**, *2*, 020502. [CrossRef]
4. Wang, Z.; Xiao, Y.; Wang, S.; Yanyuan, S.; Wang, B.; Chen, Y.; Zhou, Z.; He, J.; Yang, L. Probabilistic shaping based constellation encryption for physical layer security. *Opt. Express* **2021**, *29*, 17890–17901. [CrossRef] [PubMed]
5. Zhao, A.; Jiang, N.; Liu, S.; Zhang, Y.; Qiu, K. Physical Layer Encryption for WDM Optical Communication Systems Using Private Chaotic Phase Scrambling. *J. Lightwave Technol.* **2021**, *39*, 2288–2295. [CrossRef]
6. Roberts, D.A.; Yoshida, B. Chaos and complexity by design. *J. High Energy Phys.* **2017**, *2017*, 121. [CrossRef]
7. Zheng, J.; Hu, H.; Xia, X. Applications of symbolic dynamics in counteracting the dynamical degradation of digital chaos. *Nonlinear Dyn.* **2018**, *94*, 1535–1546. [CrossRef]
8. Chen, S.; Liu, B.; Mao, Y.; Ren, J.; Song, X.; Ullah, R.; Zhao, D.; Jiang, L.; Han, S.; Zhao, J.; et al. Physical layer data encryption using two-level constellation masking in 3D-CAP-PON. *Chin. Opt. Lett.* **2021**, *19*, 010601. [CrossRef]
9. Ren, L.; Guo, R.; Vincent, U. Coexistence of synchronization and anti-synchronization in chaotic systems. *Arch. Control Sci.* **2016**, *26*, 69–79. [CrossRef]
10. Cui, M.; Chen, Y.; Zhang, C.; Liang, X.; Wu, T.; Liu, S.; Wen, H.; Qiu, K. Chaotic RNA and DNA for security OFDM-WDM-PON and dynamic key agreement. *Opt. Express* **2021**, *29*, 25552–25569. [CrossRef] [PubMed]
11. Tang, R.; Ren, J.; Fang, J.; Mao, Y.; Han, Y.; Shen, J.; Zhong, Q.; Wu, X.; Tian, F.; Liu, B. Security strategy of parallel bit interleaved FBMC/OQAM based on four-dimensional chaos. *Opt. Express* **2021**, *29*, 24561–24575. [CrossRef] [PubMed]
12. Li, Y.; Li, C.; Zhang, S.; Chen, G.; Zeng, Z. A Self-Reproduction Hyperchaotic Map with Compound Lattice Dynamics. *IEEE Trans. Ind. Electron.* **2022**, *69*, 10564–10572. [CrossRef]
13. Ke, J.; Yi, L.; Yang, Z.; Yang, Y.; Zhuge, Q.; Chen, Y.; Hu, W. 32 Gb/s chaotic optical communications by deep-learning-based chaos synchronization. *Opt. Lett.* **2019**, *44*, 5776–5779. [CrossRef] [PubMed]
14. Ren, J.; Liu, B.; Zhao, D.; Han, S.; Chen, S.; Mao, Y.; Wu, Y.; Song, X.; Zhao, J.; Liu, X.; et al. Chaotic constant composition distribution matching for physical layer security in a PS-OFDM-PON. *Opt. Express* **2020**, *28*, 39266–39276. [CrossRef] [PubMed]
15. Zhang, W.; Zhang, C.F.; Chen, C.; Zhang, H.J.; Qiu, K. Brownian Motion Encryption for Physical Layer Security Improvement in CO-OFDM–PON. *IEEE Photonics Technol. Lett.* **2017**, *29*, 1023–1026. [CrossRef]
16. Zhang, C.F.; Zhang, W.; He, X.J.; Chen, C.; Zhang, H.J.; Qiu, K. Physically secured optical OFDM-PON by employing chaotic pseudorandom RF subcarriers. *IEEE Photonics J.* **2017**, *9*, 7204408. [CrossRef]
17. Mushenko, A.; Dzuba, J.; Nekrasov, A.; Fidge, C. A Data Secured Communication System Design Procedure with a Chaotic Carrier and Synergetic Observer. *Electronics* **2020**, *9*, 497. [CrossRef]
18. Shao, W.; Cheng, M.; Deng, L.; Yang, Q.; Dai, X.; Liu, D. High-speed secure key distribution using local polarization modulation driven by optical chaos in reciprocal fiber channel. *Opt. Lett.* **2021**, *46*, 5910–5913. [CrossRef]
19. Fu, Y.; Cheng, M.; Shao, W.; Luo, H.; Li, D.; Deng, L.; Yang, Q.; Liu, D. Analog-digital hybrid chaos-based long-haul coherent optical secure communication. *Opt. Lett.* **2021**, *46*, 1506–1509. [CrossRef]
20. Zhao, Z.; Cheng, M.; Luo, C.; Deng, L.; Zhang, M.; Fu, S.; Tang, M.; Shum, P.; Liu, D. Semiconductor-laser-based hybrid chaos source and its application in secure key distribution. *Opt. Lett.* **2019**, *44*, 2605–2608. [CrossRef] [PubMed]