Multi-Domain Multi-Level Optical Encryption Transmission Scheme Based on Memristor Rulkov Neuron Chaos

Zhiruo Guo, Bo Liu, Jianxin Ren, Qing Zhong, Yaya Mao, Xiangyu Wu, Wenchao Xia, Xiumin Song, Shuaidong Chen, Ying Li, Feng Wang, and Yongfeng Wu

***Abstract*—This paper proposes a multi-domain multi-level (MDML) orthogonal frequency division multiplexing (OFDM) optical encryption transmission scheme based on memristor Rulkov neuron chaos. In this scheme, the masking factors generated by the memristor Rulkov neuron chaos are used to encrypt the information of the digital modulation process, so as to improve the anti-malicious attack performance of the system. Among them, the memristor unit constructs a simple discrete map to capture the complex nonlinear neuronal behavior, and the generated masking factors encrypt the data in the digital modulation process. In addition, the proposed scheme introduces the encryption depth control parameters (EDCP), which can make up for the information damage caused by the complexity of encryption. The selection of EDCP can not only encrypt the data, but also change the distribution of the uniformly distributed constellation points position, reduce the average power of the constellation points, and improve the transmission performance of the fiber communication system. A 9.41 Gb/s OFDM signal transmission over 25 km standard single-mode fiber (SSMF) is experimentally demonstrated. The introduction of memristor Rulkov neurons makes the key space reach 10^{116}. The introduction of the EDCP makes the key space expand 10^{36} times. When the bit error rate (BER) is 10^{-2}, the receiving sensitivity of the EDCP with 0.2, 0.4, 0.8 is 6 dB higher than that of the EDCP with 0.9, 0.3, 0.1. The results show that the encryption scheme can effectively resist illegal attacks and improve the security performance of the system.**

***Index Terms*—Memristor Rulkov neuron chaos, chaotic encryption, physical layer security, flexible optical access.**

Manuscript received 3 July 2024; accepted 9 July 2024. Date of publication 17 July 2024; date of current version 26 August 2024. This work was supported in part by the National Key Research and Development Program of China under Grant 2021YFB2800903, in part by the National Natural Science Foundation of China under Grant U22B2009, Grant U22B2010, Grant 62225503, Grant 62205151, and Grant U2001601, in part by Jiangsu Provincial Key Research and Development Program under Grant BE2022079 and Grant BE2022055-2, in part by The Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 22KJB510031, and in part by The Startup Foundation for Introducing Talent of NUIST. *(Corresponding author: Bo Liu.)*

Zhiruo Guo, Bo Liu, Jianxin Ren, Yaya Mao, Xiangyu Wu, Wenchao Xia, Xiumin Song, Shuaidong Chen, Ying Li, Feng Wang, and Yongfeng Wu are with the Institute of Optics and Electronics, Jiangsu Key Laboratory for Optoelectronic Detection of Atmosphere and Ocean, Jiangsu International Joint Laboratory on Meteorological Photonics and Optoelectronic Detection, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: 15366061878@163.com; bo@nuist.edu.cn; 003458@nuist.edu.cn; 002807@nuist.edu.cn; 1476279183@qq.com; 20211217005@nuist.edu.cn; 003790@nuist.edu.cn; 1678612644@qq.com; ying@nuist.edu.cn; 003101@nuist.edu.cn; wuyongfeng@nuist.edu.cn).

Qing Zhong is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: zqngxs02@163.com).

Digital Object Identifier 10.1109/JPHOT.2024.3429238

I. Introduction

With the continuous development of optical networks and modern communication technologies, new network services such as digital twins, virtual reality/augmented reality, and meta-universe are emerging. More and more devices are connected to the Internet, and the traffic of the communication network shows an explosive growth trend [1], [2]. Orthogonal frequency division multiplexing (OFDM) has been widely studied in optical communication because of its high spectral efficiency, high robustness to channel dispersion and high flexibility [3]. At the same time, due to the exponential growth of communication capacity and the increase of accessibility, there will inevitably be corresponding security risks. At present, a large number of optical communication links are deployed in financial and government business, and the security of communication systems becomes particularly important [4], [5], [6]. Therefore, increasing the information transmission capacity while effectively ensuring information security is a very important research direction for future optical communication systems.

The randomness in wireless communication systems comes from spatial multiple paths that cannot be captured by all listeners [7]. Unlike wireless communication systems, all the randomness in fiber communication systems is contained in the signals transmitted inside the fiber. Illegal personnel can cause trace optical signals to leak by bending fibers, monitoring redundant strings of adjacent channels, etc., and then achieve the purpose of cracking information [8], [9]. To solve the problem of information leakage and cracking in optical communication links, researchers have proposed different types of encryption methods. The proposed encryption methods mainly focus on the advanced encryption protocol of the network, such as the encryption protocol used in the media access control layer. However, the security encryption protocol of the upper layer has the danger of exposing the data frame header [10]. With the arrival of the era of quantum computing, the possibility of cracking the above encryption scheme has also risen rapidly [11], [12]. In contrast, the encryption of the physical layer of data can effectively improve the security of data. The encryption mode of the physical layer can transparently encrypt the data transmitted at high speed, and can adapt to the development trend of large-capacity and high-rate optical communication [13], [14], [15].

Two typical methods of physical layer encryption are quantum key distribution and chaotic encryption [16], [17]. Quantum key distribution faces certain challenges in coding, digital signal processing (DSP) and parallel operation, and it is difficult to meet the demand of large-capacity and high-rate data transmission [18]. Chaotic physical layer encryption technology is a potential solution to enhance physical layer security with the characteristics of high sensitivity, high randomness, large bandwidth and low delay of initial value [19]. Chaotic physical layer encryption is mainly divided into analog domain encryption and digital domain encryption. Analog domain encryption is an optical chaos encryption using feedback laser, which is costly and complex, and is difficult to be compatible with the existing optical communication system architecture. Digital domain chaotic encryption can be combined with DSP to realize high-speed data security transmission. The technology is highly reliable and flexible, and is compatible with existing optical communication system architectures [20], [21]. Reference [22] after the QAM constellation point distribution is disturbed, the modulated FBMC bits and symbols are interleaved and encrypted to realize the improvement of the FBMC/OQAM system physical layer security performance. A hybrid secure method based on improved deoxyribonucleic acid (DNA) encoding encryption and spiral scrambling is proposed to improve the physical layer security of chaotic OFDM-PON [23]. In reference [24], A high-security and reliable self-homodyne coherent system based on the constellation shaping technique and the digital chaos is described. The chaotic sequence is generated by a four-dimensional hyperchaotic system, which is used respectively for exclusive or operation, chaotic constant composition distribution matching, phase perturbation and optical layer delay perturbation. In addition, some researchers convert the two sequences originally used to generate artificial noise into a set of phase rotation keys and complex conjugate keys, so that the encrypted symbols are still on the ideal constellation point coordinates, and realizes a sign-level encryption scheme based on phase ambiguity [25]. All the above encryption schemes avoid the cohesive operation of constellation points to achieve encryption, because the cohesive encryption of constellation points will seriously damage the transmission performance. At present, no suitable scheme has been developed to alleviate the transmission damage caused by cohesive encryption.

The study of neurodynamics is the key to unravel the mystery of brain function and neural network behavior. In this context, Rukov neurons have become a fascinating area of research due to their special ability to describe nonlinear neuronal activity [26], [27]. Rulkov neurons represent a unique class of nonlinear neuron models originally proposed by Russian scientist Andrei Rulkov in 2002 [28], [29], [30]. What sets them apart is their ability to capture complex neuronal behavior using simple discrete mapping, while also simulating key features of biological neurons such as subthreshold oscillations, spike behavior, and pulse generation. This elegant and powerful modeling approach has made discrete Rulkov neurons an important tool in neuroscience research and computational neuroscience [31], [32]. The purpose of this paper is to study the dynamic properties of discrete Rulkov neurons and explore their potential applications in the field of optical communication encryption.

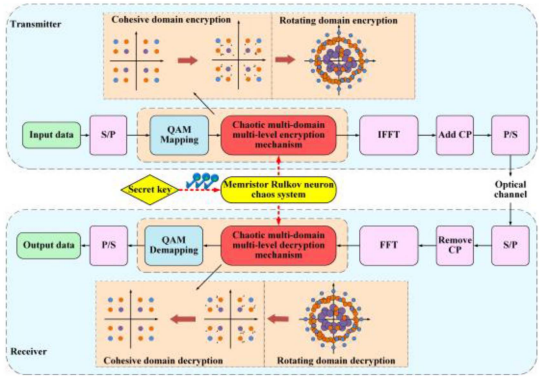

Fig. 1. Schematic diagram of MDML encryption mechanism based on memristor Rulkov neuron chaos.

In this paper, a multi-domain multi-level (MDML) encryption transmission scheme based on memristor Rulkov neuron chaos is proposed. In this scheme, the chaotic sequences generated by the chaotic system of memristor Rulkov neurons are used to encrypt the information of the cohesive domain and the rotating domain. The chaotic system of memristor Rulkov neurons maps x and z sequences to encrypt the cohesive domain constellation points. We carry out hierarchical encryption in the process of cohesive domain encryption. Taking 16QAM as an example, it is divided into three levels of encryption according to the amplitude of constellation points. In the scheme, encryption depth control parameters (EDCP) k_1, k_2 and k_3 are introduced to change the position of three-levels constellation points of 16QAM respectively. When the bit error rate (BER) is 10^{-2}, the receiving sensitivity of the EDCP with 0.2, 0.4, 0.8 is 6 dB higher than that of the EDCP with 0.9, 0.3, 0.1. Therefore, the scheme can change the distribution position of the uniformly modulated constellation without serious damage to the transmission performance, and enhance the signal and noise immunity. The chaotic system of Rulkov neurons maps y sequences to encrypt the rotating domain and realize 100% scrambling of constellation points. The key space of the proposed scheme reaches 10^{116}. The proposed scheme is verified in a 25 km standard single-mode fiber (SSMF) transmission system with a rate of 9.41 Gb/s, and the performance of the system is analyzed. The results show that when the EDCP are $k_1 = 0.9$, $k_2 = 0.3$, $k_3 = 0.1$, the performance of the encryption system is significantly lower than that when EDCP are $k_1 = 0.2$, $k_2 = 0.4$, $k_3 = 0.8$. The proposed scheme can enhance both transmission performance and security performance, and has a good prospect in the future physical layer security optical network.

II. Principles

Fig. 1 shows the principle of the MDML encryption transmission scheme based on memristor Rulkov neuron chaos, which shows the schematic presentation of cohesive domain encryption and rotating domain encryption. The cohesive domain encryption means that the constellation points of the outer part are clustered towards the middle point by chaotic sequence mapping, and the number and degree of the constellation points are randomly controlled by the chaotic sequence. Rotating domain

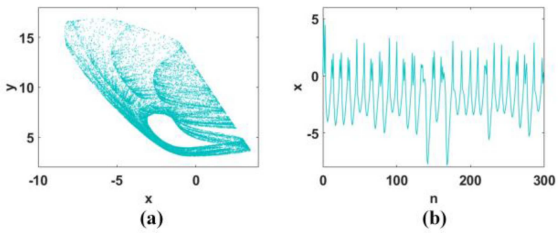

Fig. 2. Typical dynamics of the map-based memristive neuron under (x_0, y_0, z_0) = (0.1, 0.1, 0.1), where (a)–(b) with $a = 5$, $b = 0.7$.

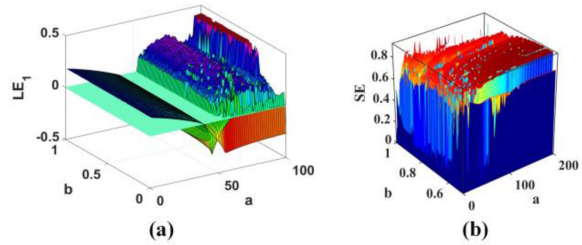

Fig. 3. The dynamical feature of the memristive Rulkov model with (x_0, y_0, z_0) = (0.1, 0.1, 0.1), (a) sample entropy, (b) maximum Lyapunov exponent.

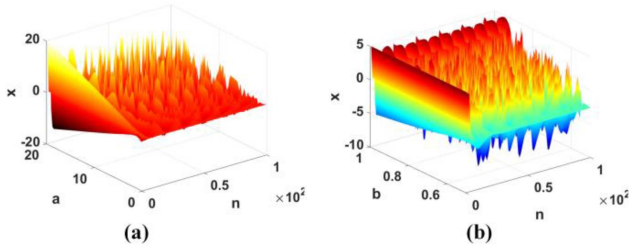

Fig. 4. The firing oscillation of the memristive Rulkov model with (x_0, y_0, z_0) = (0.1, 0.1, 0.1).

encryption refers to the use of chaotic sequence mapping to mask the phase information of constellation points.

At the transmitter, the pseudo-random binary sequence is generated as the original input data. After the input data is encoded by serial-to-parallel (S/P) conversion and constellation mapping, the masking factor generated by the key-driven memristor Rulkov neuron chaos system is used to encrypt the data. Firstly, the constellation points with different amplitudes are hierarchical cohesive encrypted to complete the cohesion change of constellation points. Then, all constellation points are masked by rotation so that the constellation points are 100% scrambled. Finally, the encrypted data are OFDM modulated and transmitted through SSMF system. At the receiver, the original data is obtained by the calculation method opposite to the encryption end. The keys drive the chaotic mapping of memristor Rulkov neurons and generates three chaotic vectors, which are used to determine the number of constellation points cohesive encryption, the cohesive distance and the rotation masking angle, respectively. It is worth noting that in this paper, the key is distributed in a way shared by both the transmitter and receiver.

A. Chaotic Sequence Generation

When the discrete memristor is introduced into the Rulkov model, the novel map-based memristive neuron is proposed. The model generates three chaotic sequences to encrypt the information. The expression is as follows:

$$\begin{cases} x_{n+1} = \frac{a}{1+x_n^2} - 0.5\tanh(z_n)y_n \\ y_{n+1} = 1.2y_n + bx_n \\ z_{n+1} = 1.2y_n - 0.6z_n \end{cases} \tag{1}$$

Set (x_0, y_0, z_0) = (0.1, 0.1, 0.1), chaotic bursting firing activities is observed is shown in Fig. 2. The sample entropy and maximum Lyapunov exponent with (x_0, y_0, z_0) = (0.1, 0.1, 0.1) are plotted in Fig. 3. The discrete sequences are shown in Fig. 4.

The complexity of chaotic sequences is measured by employing sample entropy [33], [34]. Set discrete sequences $\{x(n)\}$ = $x(1)$, $x(2)$, …, $x(N)$. A set of vector sequences $X_m(1)$, …, $X_m(N\text{-}m+1)$ with dimension m are extracted, where $X_m(i)$ = $\{x(i), x(i+1), \ldots, x(i+m\text{-}1)\}$, $1 \le i \le N\text{-}m+1$. The values of m consecutive x starting from point i are represented by these vectors. Define the distance $d[X_m(i), X_m(j)]$ between vectors $X_m(i)$ and $X_m(j)$ as the absolute value of the maximum difference between the corresponding elements. $d[X_m(i), X_m(j)] = \max k$ = 0, …, m-1$\{|x(i+k)\text{-}\ x(j+k)|\}$. For the given $X_m(i)$, count the number of j ($1 \le j \le N\text{-}m$, $j \ne i$) whose distance between $X_m(i)$ and $X_m(j)$ is less than or equal to r, which is defined as B_i. For $1 \le i \le$ N-m, $B_i^m(r)$is expressed as,

$$B_i^m(r) = \frac{B_i}{N-m-1} \tag{2}$$

$$B^{(m)}(r) = \frac{\sum_{i=1}^{N-m} B_i^m(r)}{N-m} \tag{3}$$

Increase the dimension to m+1, and calculate the number of distances $X_{m+1}(i)$ and $X_{m+1}(j)$ ($1 \le j \le N\text{-}m$, $j \ne i$) that are less than or equal to r, denoted as A_i. The $A_i^m(r)$ is defined as,

$$A_i^m(r) = \frac{A_i}{N-m-1} \tag{4}$$

$$A^{(m)}(r) = \frac{\sum_{i=1}^{N-m} A_i^m(r)}{N-m} \tag{5}$$

In this way, $B^m(r)$ is the probability of two sequences matching m points under similar tolerance r, while $A^m(r)$ is the probability of two sequences matching m+1 points. The sample entropy is defined as,

$$SE(m, r, N) = -\ln\left[\frac{A^m(r)}{B^m(r)}\right] \tag{6}$$

B. Encryption Mechanis

In order to ensure the security of the transmitted information, the scheme adopts the memristor Rulkov neuron chaos encryption technology to realize the physical layer encryption. The physical layer encryption scheme proposed in this scheme defines cohesive domain encryption and rotating domain encryption, as shown in Fig. 5. Cohesive domain encryption is the

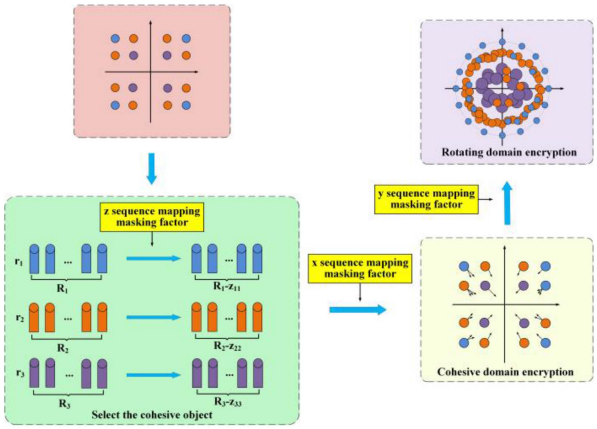

Fig. 5. Schematic diagram of MDML multilevel optical encryption mechanis.

indent encryption of constellation points towards the center by using chaotic sequence. Rotating domain encryption is to realize rotation encryption of constellation points by using chaotic sequence. It is worth noting that in the process of cohesive domain encryption, the scheme introduces the EDCP k_1, k_2, k_3, which are used to control the degree of cohesive encryption. The key consists of the initial state of the chaotic map of the memristor Rulkov neuron, the control parameter (a, b), and the EDCP k. The chaotic system of memristor Rulkov neurons generates three chaotic sequences, namely x, y, and z. The three chaotic sequences are processed into masking factors for MDML encryption. As shown in Fig. 5, the chaotic sequences x and z are used for constellation point cohesive domain encryption. The encryption method of the cohesive domain makes the constellation points no longer evenly distributed, which can reduce the average power of the constellation points. The chaotic sequences y is used for constellation point rotary domain encryption. The encryption method of the rotating field makes the constellation points achieve 100% scrambling. In addition, in the process of cohesive domain encryption, the scheme also carries out multi-level encryption. According to the different amplitude of constellation points, it is divided into three levels, and each level is successively cohesive encryption.

In the process of cohesive domain encryption, it is divided into three levels according to the amplitude of 16QAM, namely r_1, r_2, r_3, where $r_1 > r_2 > r_3$, and the three levels are successively cohesive encryption. The number of constellation points with amplitude r_1 is R_1. The number of constellation points with amplitude r_2 is R_2. The number of constellation points with amplitude r_3 is R_3. The total number of bits produced is $(R_1 + R_2 + R_3) \times 4$. Specifically, the first level of encryption encrypts constellation points with amplitude r_1. Chaotic sequence z is used to select reserved constellation points, that is, constellation points without cohesion encryption. This part of constellation points is relatively small, and most constellation points are cohesion encryption. Chaotic sequence z can not be used to select constellation points directly, it needs to be preprocessed. The specific process is as follows:

$$z_1 = |round(z \times 3601)| \tag{7}$$

$$z_{11} = sort(unique(z_1)) \tag{8}$$

where round is rounded down, unique is retained as a unique value, and sort is reordered. The number of z_{11} is much smaller than R_1.

The chaotic sequence z is preprocessed into z_{11}. The z_{11} can select constellation points of amplitude r_1, while unselected data is cohesive encrypted. The first level of cohesive encryption is to use the masking factor generated after the preprocessing of chaotic sequence x for masking. The values of the generated masking factors are all greater than 0.15 and less than 1. Constellation points with amplitude r_1 can effectively converge towards the center point when multiplied by the masking factor. It is worth noting that the masking factors generated by pretreatment should not be too small. If it is too small, the cohesive constellation point will be very close to the central origin, its coordinate is infinitely close to (00). It is difficult to recover the original constellation points when the reverse operation is performed at the receiver. This is also the reason why there is little research on constellation telescopic masking. The telescopic masking of constellation points will greatly affect the transmission performance, especially the multilevel telescopic masking. In the first level of cohesive encryption, the chaotic sequence x is preprocessed to generate masking factors. The masking factor encrypts the constellation points that need to be cohesive encrypted. The specific process is as follows:

$$x1'_i = \begin{cases} |x_i \cdot k_1| \, |x_i \cdot k_1| \geq 0.15 \\ |x_i \cdot k_1| + 0.1 \, |x_i \cdot k_1| < 0.15 \end{cases} \tag{9}$$

$$x1''_i = \begin{cases} 1i = z_{11} \\ x1'_i i \neq z_{11} \end{cases} \tag{10}$$

where k_1 is the EDCP of the first level of cohesive encryption, and its size can determine the degree of constellation point cohesion. If the value of k_1 is too small, it will be more difficult to recover at the receiver. The matrices generated by (9) are all less than 1 and greater than 0.15. The chaotic sequence is stochastic, which can be used for cohesion masking of constellation points. The function of (10) is to preserve a part of the constellation points from cohesion encryption, and its amplitude is still r_1. The selection of these constellation points is determined by z_{11}. The processed x sequence has some elements of 1 and most elements of $x1'_i$.Then the masking factor $x1'_i$ is used to cohesive encrypt the constellation points with amplitude r_1. The specific encryption process is as follows:

$$w'_i = w_i \cdot x1''_i \tag{11}$$

where w_i is the original constellation point with amplitude r_1, and w'_i is the constellation point after cohesion encryption. The second and third levels of encryption in the cohesive encryption process are similar to the first level. The chaotic sequence z is preprocessed to generate z_{22} and z_{33}. z_{22} and z_{33} select constellation points with amplitude r_2 and r_3 respectively, and mask constellation points that need cohesion encryption. The specific processing process is as follows:

$$z_2 = |round(z \times 4831)| \tag{12}$$

$$z_{22} = sort(unique(z_2)) \tag{13}$$

$$z_3 = |round(z \times 431)| \tag{14}$$

$$z_{33} = sort(unique(z_3)) \tag{15}$$

In the process of the second and third level cohesive encryption, the masking factor generated by the preprocessing of chaotic sequence x is used to encrypt the information. At the same time, the EDCP k_2 and k_3 are introduced, which determine the degree of constellation point cohesion. The specific masking factor generation process is as follows:

$$x2'_i = \begin{cases} |x_i \centerdot k_2| & |x_i \centerdot k_2| \geq 0.15 \\ |x_i \centerdot k_2| + 0.1 & |x_i \centerdot k_2| < 0.15 \end{cases} \tag{16}$$

$$x3'_i = \begin{cases} |x_i \centerdot k_3| & |x_i \centerdot k_3| \geq 0.15 \\ |x_i \centerdot k_3| + 0.1 & |x_i \centerdot k_3| < 0.15 \end{cases} \tag{17}$$

$$x2''_i = \begin{cases} 1i = z_{22} \\ x2'_i i \neq z_{22} \end{cases} \tag{18}$$

$$x3''_i = \begin{cases} 1i = z_{33} \\ x3'_i i \neq z_{33} \end{cases} \tag{19}$$

The masked constellation points can be obtained by multiplying the processed masking factors $x2''_i$ and $x3''_i$ with the coordinates of the constellation points whose amplitudes are r_2 and r_3. The specific encryption process is as follows:

$$u'_i = u_i \centerdot x2''_i \tag{20}$$

$$p'_i = p_i \centerdot x3''_i \tag{21}$$

where u_i is the constellation point with the original amplitude r_2, and u'_i is the constellation point after cohesive encryption. p_i is the original constellation point with amplitude r_3, and p'_i is the constellation point after cohesive encryption.

The chaotic sequence generated by the chaotic system in this scheme can match the numerical value in the process of digital modulation well. The traditional digital domain physical layer encryption schemes need to enlarge the chaotic sequence by 10^n order, and then obtain the usable masking factor. In this scheme, the cohesive encryption process expands the chaotic sequence up to 4831 times, which effectively reduces the amount of numerical calculation.

In the encryption process of rotating domain, the masking factor is mapped by chaotic sequence y for rotation masking of constellation points. This process can complete 100% of the constellation points scrambling. The value of the masking factor generated by the chaotic sequence y is randomly distributed between 0 and 360, which can effectively rotate the constellation points randomly between 0 and 360 degrees. The value of the masking factor is generated by taking the remainder. Its specific encryption process is as follows:

$$\begin{cases} m = floor(\mathrm{mod}(y \centerdot 10^8, 360)) \\ t' = t \cdot (\cos(m) + j \sin(m)) \end{cases} \tag{22}$$

where t is the unrotated encrypted constellation coordinate and t' is the rotated encrypted constellation coordinate.

The physical layer information encryption scheme proposed in this paper is completed in DSP, which is compatible with the existing optical network and has greater flexibility. At the receiver, data recovery only needs to be inverse operated, which can effectively decrypt and recover information.

C. System Encryption Complexity Calculation

In this paper, the computational complexity of the proposed scheme is evaluated. The complexity arises mainly from three parts. 1) The chaotic system of memristor Rulkov neurons generates chaotic sequences x, y, z. 2) The generation of masking factors z_{11}, z_{22}, z_{33}, $x1''_i$, $x2''_i$, $x3''_i$ and m. 3) The specific process of encryption. In terms of the generation of chaotic sequences x, y, z, the memristor Rulkov neuron chaotic system has 4 times addition and subtraction calculations, 1 time $\tanh(\centerdot)$ calculation, 8 times multiply and divide calculations, the number of iterations is $2 \times (R_1 + R_2 + R_3)$. In terms of the generation of masking factors z_{11}, z_{22} and z_{33}, $2 \times (R_1 + R_2 + R_3)$times multiplication and division calculations, $2 \times (R_1 + R_2 + R_3)$times absolute value calculations and $2 \times (R_1 + R_2 + R_3)$ times integer calculations are carried out respectively. The process of generating masking factor $x1''_i$ consists of R_1 times multiplication and division calculations, R_1 times absolute value calculations, R_1 times addition and subtraction calculations, and $2 \times R_1$times judgment calculations. The process of generating masking factor $x2''_i$ consists of R_2 times multiplication and division calculations, R_2 times absolute value calculations, R_2 times addition and subtraction calculations, and $2 \times R_2$times judgment calculations. The process of generating masking factor $x3''_i$ consists of R_3 times multiplication and division calculations, R_3 times absolute value calculations, R_3 times addition and subtraction calculations, and $2 \times R_3$times judgment calculations. The process of generating masking factor m consists of (R_1+R_2+R_3) times multiplication and division calculations, (R_1+R_2+R_3) times $\mathrm{mod}(\centerdot)$ calculations, and (R_1+R_2+R_3) times $flood(\centerdot)$ calculation. In terms of the specific process of encryption, the three-level encryption of the cohesive domain is carried out a total of (R_1+R_2+R_3) multiplication and division calculation. Rotating domain encryption performs (R_1+R_2+R_3) times $\cos(\centerdot)$ calculations, (R_1+R_2+R_3) times $\sin(\centerdot)$ calculations, (R_1+R_2+R_3) addition and subtraction calculations, and (R_1+R_2+R_3) multiplication and division calculations.

III. Experimental Setup and Results

A. Experimental Setup

The experimental setup of the proposed scheme is shown in Fig. 6. In order to verify the reliability of the proposed security scheme, the receiver is divided into a legal optical network unit (ONU) and an illegal ONU. Illegal OUN does not have security key and can only obtain information by brute force. The number of OFDM subcarriers is set to 512. The number of inverse fast fourier transform (IFFT) points is set to 2048. The protection interval is set to 1/16. The arbitrary waveform generator (AWG, TekAWG70002A) has a sampling rate of 50 GSa/s. The light source information wavelength is 1550 nm. The continuous wave laser has a power of 12 dBm. The mixed signal oscilloscope (MSO, TekMSO73304DX) has a sampling rate of 50 GSa/s. First, the input data is converted into an analog radio-frequency

III. Experimental Setup and Results

A. Experimental Setup

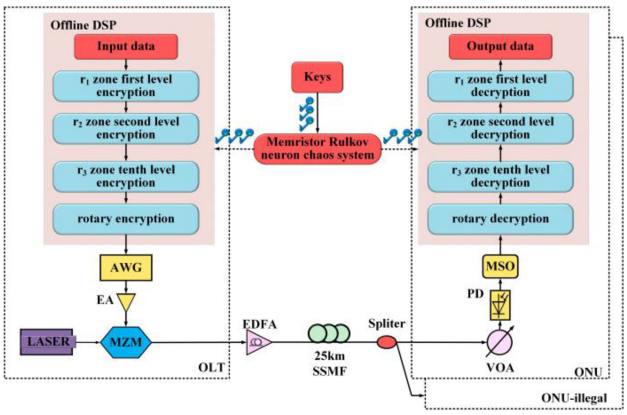

Fig. 6. Experimental setup (AWG: Arbitrary waveform generator; EA: Electrical amplifier; MZM: Mach-Zehnder modulator; EDFA: Erbium-doped fiber amplifier; VOA: Variable optical attenuator; PD: Photodiode; MSO: Mixed signal oscilloscope).

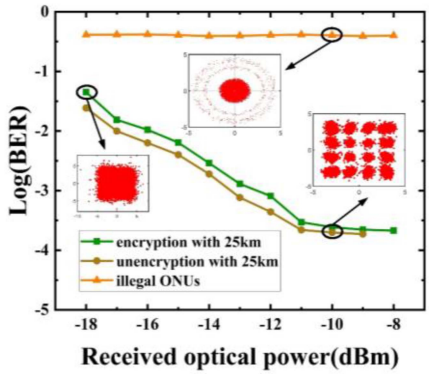

Fig. 7. BER curves of normal and illegal reception for 25 km transmission.

signal by AWG after MDML chaotic encryption. Second, the signal passes through the amplifier electrical amplifier (EA), it is loaded onto the light generated by the laser via a Mach- Zehnder modulator (MZM). Third, the optical signal is sent to the SSMF channel of 25 km for transmission. The optical signal at the receiver is converted into an electrical signal by a photodiode (PD), and then the analog-to-digital conversion is completed by an MSO. Finally, the original data is recovered by offline DSP. The function of the variable optical attenuator (VOA) is to adjust the received optical power.

B. Experimental Results and Analysis

In this paper, the bit error performance of transmission schemes under different scenarios are compared. Fig. 7 describes the BER curve and constellation diagram under normal reception and illegal reception. The normal reception includes encrypted and unencrypted cases. It can be seen from the figure that the BER of the normal receiver decreases with the increase of the received optical power. When the received optical power is greater than -11 dBm, the BER of the normal receiver is lower than 3.6×10^{-3}, and the constellation diagram is clear. When

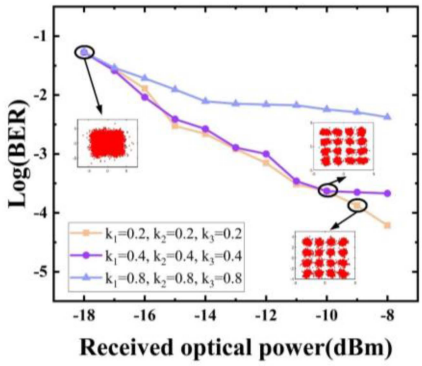

Fig. 8. BER curves of k_1, k_2, and k_3 with the same value.

the received optical power is -18 dBm, the constellation image is not clear and the BER increases. However, the BER of the illegal receiver does not change with the change of the received optical power, and is stable at about 0.4. The illegal ONU mainly mimics the behavior of an eavesdrooper, that is, parsing data without obtaining the correct key, the correct chaotic system, and the correct encryption mechanism. The illegal ONU mainly embodies the eavesdropper's behavior in the digital signal processing part, and performs brute force cracking of encrypted data without the correct key. The constellation diagram, as shown in the illustration, appears circular and cannot be decrypted. This is because the normal receiver has the same key as the transmitter to correctly decrypt information, and the illegal receiver without the correct key is unable to recover the interfered signal.

Compared with the unencrypted signal, the BER of the encrypted signal is slightly lower. The performance of the system in the case of encryption is slightly affected. However, this scheme can effectively protect the data, and the damage of transmission performance can be accepted. Therefore, the scheme guarantees the communication quality and performance, and can effectively resist illegal attacks.

The influence of EDCP on transmission performance is also tested. The value range of the EDCP k is (0, 1]. The smaller the value of k, the larger the cohesion degree of constellation points in multi-domain. The larger the value of k, the smaller the cohesion degree of the constellation points in the multi-domain. When k_1, k_2 and k_3 values are the same, the influence on the BER of the system is analyzed. The EDCP that control the cohesion degree of MDML constellation points are set the same and are respectively 0.2, 0.4 and 0.8, and the BER curves are shown in Fig. 8. As can be seen from the figure, the BER of the system under the three parameters decreases with the increase of the received optical power generally. In the case of the same received optical power, the BER of the transmission system with the EDCP value of 0.8 is larger than that of the EDCP of 0.2 and 0.4. This is because the average power is small when the EDCP is 0.2 and 0.4. Compared with the EDCP of 0.8, the transmission performance will be improved. However, it is not the case that the smaller the EDCP, the better. When the EDCP is small, the degree of constellation points contraction increases, and the difficulty of recovery will increase. When the received optical power is greater than -10 dBm, the BER of the system

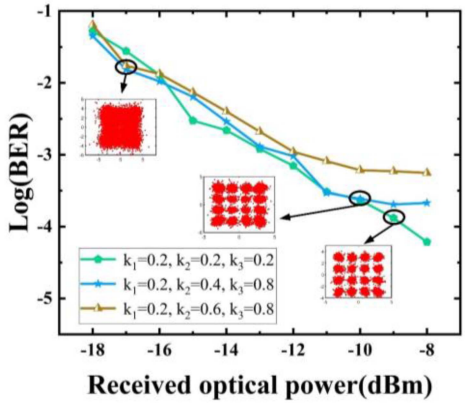

Fig. 9. BER curves with $k_1 = 0.2$ and different values of k_2 and k_3.

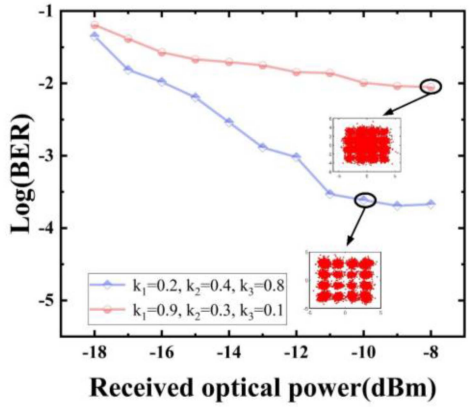

Fig. 11. BER curve with different values of k_1, k_2, and k_3.

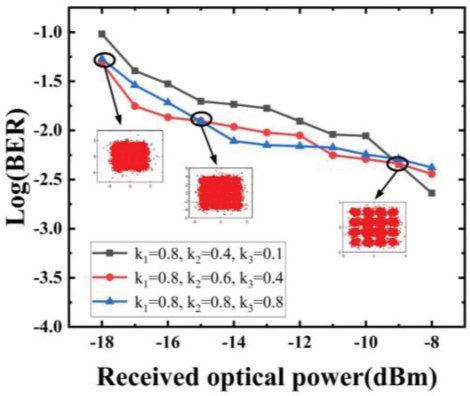

Fig. 10. BER curves with $k_1 = 0.8$ and different values of k_2 and k_3.

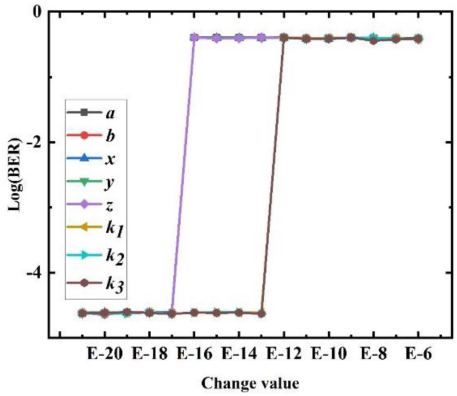

Fig. 12. BER curves of various ONUs with a tiny change in initial value.

whose EDCP k_1, k_2 and k_3 are all 0.4 is lower than 2×10^{-4}. When the EDCP k_1, k_2 and k_3 are all 0.2, the BER of the system is lower than 2.1×10^{-4}. The constellation diagram is shown in the illustration with the constellation points clearly visible.

In addition, the system test is carried out when the EDCP k_1 is the same and small, and the EDCP k_2 and k_3 are different. k_1 is fixed at 0.2, the EDCP of constellation points in other domains are adjusted under MDML, and then the influence of different k on the BER of the system is analyzed. When the received optical power is less than -17 dBm, as shown in the illustration in Fig. 9, the constellation diagram is not clear and the BER increases. With the increase of optical power, the BER decreases. When the received optical power is less than -10 dBm, the constellation diagram is clear. In addition, it can be seen from the figure that under the same received optical power, the BER of $k = (0.2, 0.2, 0.2)$ is the lowest, and the BER of $k = (0.2, 0.6, 0.8)$ is the highest. The selection of EDCP has a great influence on the transmission performance of the system. The introduction of the EDCP variable makes the encryption system more complex, and the difficulty for eavesdroppers to steal information increases.

Different from the test in Fig. 9, the result of the BER in Fig. 10 is to increase the value of the EDCP k_1. k_1 is fixed at 0.8, the EDCP of constellation points in other domains are adjusted under MDML. Compared with the results in Fig. 9, when the EDCP k_1 is set to 0.8, the transmission performance is significantly lower than that when the EDCP k_1 is 0.2, and the signal is seriously damaged. When the received optical power is less than -18 dBm, as shown in the illustration, the constellation diagram appears as a cluster, very unclear, and the BER increases. When the received optical power is greater than -15 dBm, the constellation diagram shows the general outline. As can be seen from the figure, under the same received optical power, the BER of $(k_1, k_2, k_3) = (0.8, 0.6, 0.1)$ is the highest, and the BER of $(k_1, k_2, k_3) = (0.8, 0.6, 0.4)$ is not much different from that of $(k_1, k_2, k_3) = (0.8, 0.8, 0.8)$.

The EDCP k_1, k_2 and k_3 are used to control the cohesion degree of constellation points of different levels respectively. The EDCP from the outer domain to the inner domain are set to 0.2, 0.4, 0.8 and 0.9, 0.3, 0.1 respectively, and the BER curve is shown in Fig. 11. As can be seen from the figure, when $(k_1, k_2, k_3) = (0.9, 0.3, 0.1)$, its transmission performance is much lower than that when $(k_1, k_2, k_3) = (0.2, 0.4, 0.8)$. Therefore, the selection of appropriate EDCP can not only ensure the transmission performance of the system, but also ensure the physical layer security of data. When the BER is 10^{-2}, the receiving sensitivity of the EDCP with 0.2, 0.4, 0.8 is 6 dB higher than that of the EDCP with 0.9, 0.3, 0.1.

In order to verify the sensitivity of the key in this scheme, this paper analyzes the BER curve after the key used to decrypt the ONU at the receiver is slightly changed. As shown in Fig. 12,

the horizontal coordinate indicates how finely the initial value changes the parameter. Take parameter z as an example, when the precision of the parameter is E-17, the BER is low, and it can be decrypted normally. When the precision of the parameter is changed to E-16, the BER increases sharply and can not be decrypted normally. This shows that the key in our scheme has a very high sensitivity. The key space can be expressed as (a, b, x, y, z, k_1, k_2, k_3), which can realize the key space of $[(10^{16})^5 \times (10^{12})^3] = 10^{116}$. Therefore, the chaotic sequence of memristor Rulkov neurons has high sensitivity. It is difficult for the thief to extract the original data from it, which has high security.

IV. Conclusion

Based on the memristor Rulkov neuronal chaotic encryption technique, this paper proposes an encryption scheme which integrates data encryption and constellation points distribution position change. The scheme uses the memristor Rulkov neuron chaos encryption model and encryption mechanism to realize information encryption and distribution position change of constellation points, which effectively realizes information security transmission and improves system transmission performance. The scheme is verified by experiments by the signal transmission of 9.41 Gb/s in a 25 km SSMF system. The experimental results show that the key in the proposed scheme has high sensitivity. The key space is up to 10^{116}, which can resist illegal attacks. When the BER is 10^{-2}, the receiving sensitivity of the EDCP 0.2, 0.4, 0.8 is 6 dB higher than that of the EDCP 0.9, 0.3, 0.1. In conclusion, the MDML encryption transmission scheme based on memristor Rulkov neuron chaos proposed in this paper has great potential in future high-security and high-speed large-capacity transmission systems.

References

[1] R. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini, and B. Goebel, "Capacity limits of optical fiber networks," *J. Lightw. Technol.*, vol. 28, no. 4, pp. 662–701, Feb. 2010.

[2] Q. Zhong et al., "Block compressive sensing chaotic embedded encryption for MCF-OFDM transmission system," *Opt. Express*, vol. 30, no. 12, pp. 21774–21786, 2022.

[3] M. Chen et al., "Experimental demonstration of an IFFT/FFT size efficient DFT-spread OFDM for short reach optical transmission systems," *J. Lightw. Technol.*, vol. 34, no. 9, pp. 2100–2105, May 2016.

[4] Z. Wei, W. Guo, and B. Li, "A multi-eavesdropper scheme against RIS secured LoS-dominated channel," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1221–1225, Jun. 2022.

[5] Y. Wu, Y. Yu, Y. Hu, Y. Sun, T. Wang, and Q. Zhang, "Channel-based dynamic key generation for physical layer security in OFDM-PON systems," *IEEE Photon. J.*, vol. 13, no. 2, Apr. 2021, Art. no. 7900209.

[6] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Physical-layer security against known/chosen plaintext attacks for OFDM-based VLC system," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2606–2609, Dec. 2017.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[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, 2019.

[9] W. Hu, Z. Wei, S. Popov, M. Leeson, and T. Xu, "Tapping eavesdropper designs against physical layer secret key in point-to-point fiber communications," *J. Lightw. Technol.*, vol. 41, no. 5, pp. 1406–1414, Mar. 2023.

[10] L. Gao, L. Zhang, and M. Ma, "Low cost RFID security protocol based on rabin symmetric encryption algorithm," *Wireless Pers. Commun.*, vol. 96, no. 1, pp. 683–696, 2017.

[11] H. Wang et al., "Performance analysis for OFDM-based multi-carrier continuous-variable quantum key distribution with an arbitrary modulation protocol," *Opt. Exp.*, vol. 31, no. 4, pp. 5577–5592, 2023.

[12] R. Goncharov et al., "Security of plug-and-play continuous-variable quantum key distribution," *J. Opt. Technol.*, vol. 89, no. 7, pp. 430–433, 2022.

[13] P. Song, Z. Hu, and C. Chan, "Multi-band chaotic non-orthogonal matrix-based encryption for physical-layer security enhancement in OFDM-PONs," *J. Opt. Commun. Netw.*, vol. 15, no. 7, pp. c120–c128, 2023.

[14] A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, "Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling," *J. Lightw. Technol.*, vol. 39, no. 8, pp. 2288–2295, Apr. 2021.

[15] Z. Wang et al., "Probabilistic shaping based constellation encryption for physical layer security in OFDM RoF system," *Opt. Exp.*, vol. 29, no. 12, pp. 17890–17901, 2021.

[16] K. Wang et al., "40 Gbits−1 data transmission in an installed optical link encrypted using physical layer security seeded by quantum key distribution," *J. Lightw. Technol.*, vol. 39, no. 19, pp. 6130–6141, Oct. 2021.

[17] M. Bi et al., "A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON," *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 7901510.

[18] T. A. Eriksson et al., "Challenges in coding, DSP and parallel operation of quantum key distribution and coherent data transmission," in *Proc. Eur. Conf. Opt. Commun.*, 2020, pp. 1–4.

[19] Q. Zhong et al., "Self-propagated chaotic dynamically enhanced optical physical layer encryption communication system based on bidirectional long short-term memory neural network," *Opt. Exp.*, vol. 30, no. 20, pp. 36379–36393, 2022.

[20] Q. Zhong et al., "High-security UFMC optical transmission system of seven-core fiber based on updating the 3D discrete chaotic model," *Opt. Lett.*, vol. 47, no. 9, pp. 2254–2257, 2022.

[21] Y. Zhang et al., "Security enhancement in coherent OFDM optical transmission with chaotic three-dimensional constellation scrambling," *J. Lightw. Technol.*, vol. 40, no. 12, pp. 3749–3760, Jun. 2022.

[22] R. Tang et al., "Security strategy of parallel bit interleaved FBMC/OQAM based on four-dimensional chaos," *Opt. Exp.*, vol. 29, no. 15, pp. 24561–24575, 2021.

[23] Y. Xiao, Y. Chen, C. Long, J. Shi, J. Ma, and J. He, "A novel hybrid secure method based on DNA encoding encryption and spiral scrambling in chaotic OFDM-PON," *IEEE Photon. J.*, vol. 12, no. 3, Jun. 2020, Art. no. 7201215.

[24] Y. Chen, J. Chen, M. Zhang, W. Li, D. Liu, and M. Tang, "High-security constellation shaped self-homodyne coherent system with 4-D joint encryption," *Opt. Exp.*, vol. 31, no. 2, pp. 3153–3167, 2023.

[25] X. Wang et al., "Chaotic physical layer encryption scheme based on phase ambiguity for a DMT system," *Opt. Exp.*, vol. 30, no. 9, pp. 14782–14797, 2022.

[26] M. Mehrabbeil, F. Parastesh, J. Ramadoss, K. Rajagopal, H. Namazi, and S. Jafari, "Synchronization and chimera states in the network of electrochemically coupled memristive Rulkov neuron maps," *Math. Biosciences Eng.*, vol. 18, no. 6, pp. 9394–9409, 2021.

[27] J. Ma and J. Tang, "A review for dynamics in neuron and neuronal network," *Nonlinear Dyn.*, vol. 89, no. 3, pp. 1569–1578, 2017.

[28] K. Li, H. Bao, H. Li, J. Ma, Z. Hua, and B. Bao, "Memristive Rulkov neuron model with magnetic induction effects," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1726–1736, Mar. 2022.

[29] Y. Li, C. Li, T. Lei, Y. Yang, and G. Chen, "Offset boosting-entangled complex dynamics in the memristive Rulkov neuron," *IEEE Trans. Ind. Electron.*, vol. 71, no. 8, pp. 9569–9579, Aug. 2024.

[30] Y. Li et al., "A memristive chaotic map with only one bifurcation parameter," *Nonlinear Dyn.*, vol. 112, no. 5, pp. 3869–3886, 2024.

[31] B. Bao, J. Hu, J. Cai, X. Zhang, and H. Bao, "Memristor-induced mode transitions and extreme multistability in a map-based neuron model," *Nonlinear Dyn.*, vol. 111, no. 4, pp. 3765–3779, 2023.

[32] H. Bao, Z. Hua, W. Liu, and B. Bao, "Discrete memristive neuron model and its interspike interval-encoded application in image encryption," *Sci. China Technological Sci.*, vol. 64, no. 10, pp. 2281–2291, 2021.

[33] Y. Li et al., "Coexisting hollow chaotic attractors within a steep parameter interval," *Chaos, Solitons Fractals*, vol. 179, 2024, Art. no. 114406.

[34] Y. Li, C. Li, S. Zhang, G. Chen, and Z. Zeng, "A self-reproduction hyperchaotic map with compound lattice dynamics," *IEEE Trans. Ind. Electron.*, vol. 69, no. 10, pp. 10564–10572, Oct. 2022.