High-Security OFDM-OAM Optical Transmission Scheme Based on Quad-Wing Ultra-Chaotic Encryption

Hao Wang, Bo Liu, Zeqian Guo, Yibin Wan, Shuyu Zhou, Zhongwen Ding, and Jianxin Ren

***Abstract*—We propose a high-security hyperchaotic orthogonal frequency division multiplexing (OFDM) encryption scheme based on the orbital angular momentum system, and our research focuses on the security and high-order modulation of the orbital angular momentum (OAM)system. In order to effectively prevent violent decryption by eavesdroppers, we adopt a high security Zhan's hyperchaotic model. In the experiments, the high security performance of the proposed encryption scheme is verified by the OAM optical transmission platform, the proposed encryption scheme has a large key space of 10^{191}, and it is demonstrated that the high-order spatial optical modulation has a small impact on the bit error rate (BER) of the OAM system within the forward error correction (FEC) threshold. The experimental results show that the proposed encryption scheme significantly improves the security performance of OAM spatial optical transmission, and is a promising candidate for the next-generation high-security OAM high-order multiplexed transmission system.**

***Index Terms*—Hyperchaos, high security, orbital angular momentum, OFDM.**

I. Introduction

With the development of modern mobile communication technology, the orthogonal frequency division multiplexing (OFDM) technology has been receiving special attention in the field of optical communication due to its advantages of high spectral efficiency, reduced multipath interference and large capacity. But the traditional multiplexing technology focusing on time, frequency and space has almost reached the limit, the explosive increase in smart terminal devices has led to a dramatic increase in the demand for channel capacity in wireless communication systems [1]. To meet the increasing demand for communication capacity, a new multiplexed communication technology is urgently needed. Orbital Angular Momentum (OAM), as one of the potential technologies in the 6th Generation (6G) mobile networks, and its orthogonality between different integer modes, allows wireless communication systems to greatly increase the system channel capacity without relying on resources such as time, space and frequency, this provides a new option to solve the resource shortage problem faced by current wireless communication systems [2]. Therefore, OAM has been studied by many scholars and institutions in the field of wireless communication.

In recent years, OAM has been extensively studied and widely used in wireless and wired communication systems [3], [4], [5] Wang et al. proposed and implemented a multiplexed demultiplexed 42.8×4 Gbit/s quadrature amplitude modulation (QAM) signal coded with different OAM values for four beams, which greatly enhanced the channel capacity [6]. Song et al. experimented with simultaneous OAM mode demul-tiplexing using a multiplanar optical converter (MPLC) [7]. But accordingly, the improvement of communication capacity and the increase of access users have brought huge challenges to data security, which has led to the widespread concern of the physical layer encryption technology of OAM system. At the same time, in free space optical communication (FSO), light propagation through the atmosphere is subject to reflection, refraction and scattering phenomena, which can easily be hijacked by illegal optical network units (ONUs), resulting in data loss.

Therefore, it is necessary to address the issue of reliable security in OAM systems. Chaotic systems are widely used in cryptographic schemes because of their good unpre-dictability, high randomness and high sensitivity to initial values [8]. With the rapid development of high-speed digital signal processing (DSP) capabilities, chaotic digitisation has also become a hot research topic. Chaotic systems are widely used in the study of optical communications due to their huge parameter space and obvious pseudo-random properties, and are easy to integrate with DSP technology [9]. In [10], secure data encryption is provided by using the chaotic Walsh-Hadamard transform. Chaotic I and Q scrambling is done in the physical layer to enhance physical layer security [11]. In [12], Deoxyribonucleic acid (DNA) coding rules are applied to user data for encryption and decryption in order to provide secure transmission, which is optimised by combining the I and Q parts of different QAM symbols. However, in all these schemes, the target mapping has equally probable and equally spaced constellation points, so that the mapping is fixed and the QAM symbols are scrambled between fixed

Manuscript received 8 December 2022; revised 27 December 2022; accepted 20 January 2023. Date of publication 24 January 2023; date of current version 21 February 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 61835005 and in part by The Startup Foundation for Introducing Talent of NUIST. *(Corresponding author: Bo Liu.)*

Hao Wang is with the Department of Engineering, Peoples Liberation Army Engineering University, Nanjing, CO 210000, China (e-mail: haowangaeu@163.com).

Bo Liu, Zeqian Guo, Yibin Wan, Shuyu Zhou, Zhongwen Ding, and Jianxin Ren are with the Institute of Optics and Electronics, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: bo@nuist.edu.cn; 1281199482@qq.com; 254547694@qq.com; 2564098462@qq.com; 20211249504@nuist.edu.cn; 003458@nuist.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2023.3239612

location points of the QAM constellation. Due to the inflexible constellation mapping, the security they provide is inade-quate. A microscopic particle-based Brownian motion-based chaotic sequence generation technique is proposed in [13] to perturb the I and Q of QAM symbols. In [14], the target mapping is made dynamic by rotating the constellation points along the radial axis. However, this flexibility in mapping QAM symbols still has a fixed radial axis and thus makes the user data of all schemes vulnerable to attacks due to statistical analysis [15]. And as the QAM symbols rotate, the Euclidean geometric distance between constellation points increases, so more symbols are needed to model noise-like con-stellations. Traditional chaotic models are less secure due to the relatively low dimensionality of the chaotic mapping [16]. In [17], The QAM symbol sequence is divided into several sub sequences, and further probability shaping (PS) is performed by constellation region replacement according to the corresponding statistical information (SI). Then the sequence SI is encoded and encrypted into chaotic signals by using the key distribution algorithm. These models have a simple structure with a small key space and are vulnerable to brute force attacks. In addition, traditional integral order-based models are computed by linear iterative equation calculations, which always require a large amount of computational resources, which may impose a very complex burden on the communication system. Therefore, for efficient encryption schemes, dynamic mapping of QAM symbols with low power cost is required. There is a lack of cryptographic coding modulation methods to ensure the reliability and security of OFDM-OAM systems.

In this article, a high-security 16QAM-OFDM-OAM spatial optical communication based on hyperchaotic four dimensional perturbation is proposed and demonstrated in an intensity modulation and direct detection (IMDD) system complete with a digital implementation of OFDM using fast Fourier transform (FFT) to generate a four-dimensional chaotic sequence from the Zhan four-wing hyperchaotic system [18] to complete the bitstream XOR encryption, constellation map rotation, and subcarrier and symbol of the permutation disturbance. The four-dimensional joint perturbation of the hyperchaotic model can significantly increase the key space and achieve highly secure message transmission. The proposed encryption scheme significantly improves the security performance of optical transmission in OAM space, and verifies the feasibility of the scheme proposed in this article.

II. Principles

The main framework of a high-security 16QAM-OFDM-OAM based on the proposed encryption scheme is shown in Fig. 1. The number of subcarriers is 256, the number of symbols is 20, and the number of FFT points is 1024. In the transmitter side of the 16QAM-OFDM-OAM system, a pseudo-random binary sequence (PRBS) generated by the DSP is used as the original input data. The 16QAM mapped constellation modulation is encrypted by the constellation mask vector by rotating the constellation points. In addition, the OFDM modulation is implemented using an inverse fast fourier transform (IFFT) matrix and the subcarrier and symbols are encrypted using a

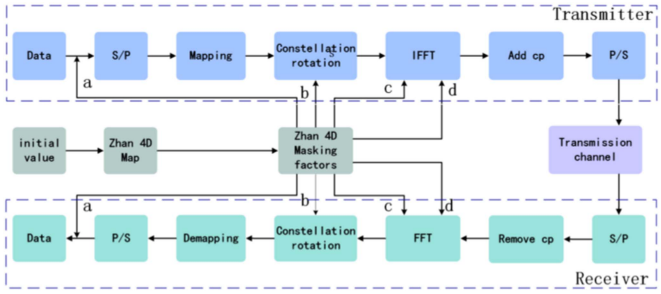

Fig. 1. Proposed 16QAM-OFDM-OAM four-dimensional perturbation encryption scheme.

frequency masking vector. Finally, we add a cyclic prefix and the encrypted signal is converted to a single-channel real signal for transmission via parallel-to-serial (P/S) conversion. The transmission enters a free-space optical communication system (FSO), where a positive-phase spatial light modulator (SLM) modulates into an OAM beam for transmission at the transmitter side, and a negative-phase SLM couples into the fibre at the receiver side to decrypt it. The original signal bit stream can be obtained by decoding and decrypting it in the opposite steps to the transmitter side.

A. Modulation and Demodulation of the Angular Momentum of OAM Orbits

OAM multiplexing technology can increase information transmission capacity and improve spectral efficiency. OAM can provide new degrees of freedom for free-space communication, as the carrier of OAM, each photon of OAM can carry an infinite amount of information. The topological charge number of OAM takes a value that is theoretically infinite, and during transmission, OAMs with different topological charge numbers are independent eigenstates that are orthogonal to each other in free-space propagation that do not affect each other [19].

The light waves of a Gaussian beam in free space can be represented by the near-axis fluctuation equation [20], which can be implemented in the course of experiments by LaguerreGauss (LG):

$$U(r,\theta,z)=\sqrt{\frac{2p!}{\pi(p+|l|)}}\frac{1}{\omega(z)}\left[\frac{r\sqrt{2}}{\omega(z)}\right]^{|l|}L_p^l\left[\frac{2r^2}{\omega^2(z)}\right]\times\exp\left[\frac{-r^2}{\omega^2(z)}\right]\exp\left[\frac{-\mathrm{i}kr^2z}{2(z^2+z_R^2)}\right]\times\exp\left[\mathrm{i}(2p+|l|+1)\arctan\frac{z}{z_R}\right]\exp(-il\theta) \tag{1}$$

In (1) denotes the OAM topological charge number denotes the number of spin angular momentum modes denotes the radial distance to the central axis is the angular coordinate is the transmission distance denotes the Rayleigh distance denotes the wave number denotes the radius of the bundle denotes the concatenated Laguerre polynomial denotes the spiral phase factor. When when denotes zero-order Gaussian light. Through the Laguerre

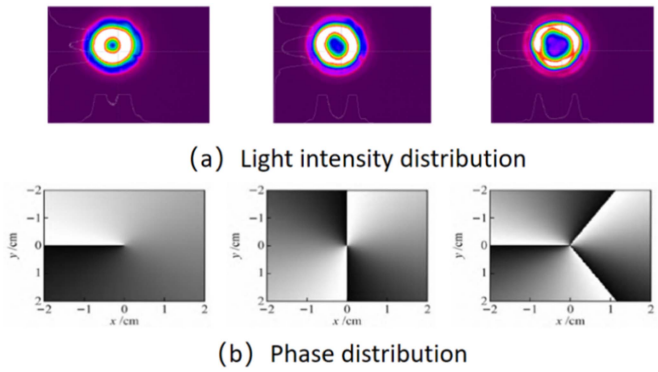

Fig. 2. Light intensity distribution and phase distribution of the LG beam (z = 0, m, p = 0) in free space light.

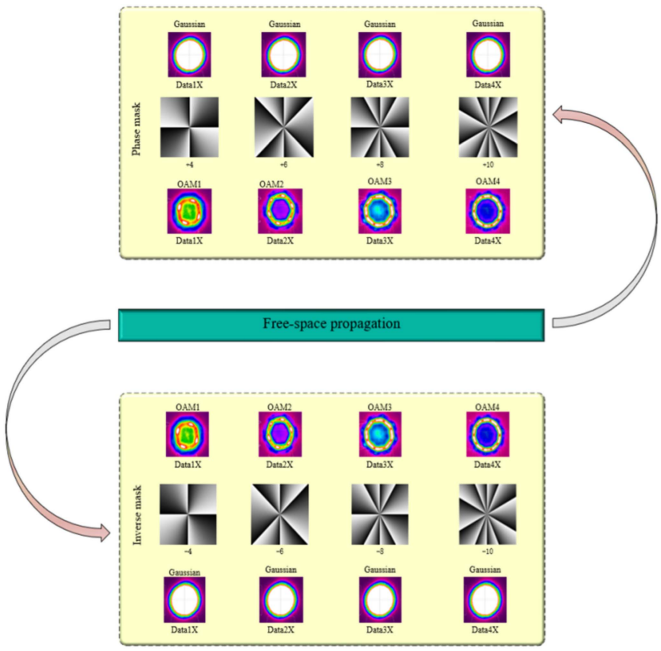

Fig. 3. Higher order modulation/demodulation of OAM beams.

Gauss formula we can learn that normal electromagnetic waves carrying normal data information can be generated by Gaussian light from the OAM beam, according to the azimuthal angle change, adding the corresponding phase rotation, making the electromagnetic waves originally sent in the same phase in a plane distorted to form an electromagnetic vortex wave [21]. the orbital angular momentum characteristics of the OAM beam are jointly determined, as shown in Fig. 2, when the light intensity and phase distribution at the light source when the beam intensity is distributed as 1 outer ring.

A conceptual diagram of OAM beam modulation/demodulation is shown in Fig. 3. In optical communications, OAM can be considered as an additional degree of freedom, and multiplexing of OAM beams carrying information provides another dimension for improving the capacity and spectral efficiency of the communication link. Capacity and spectral efficiency can be

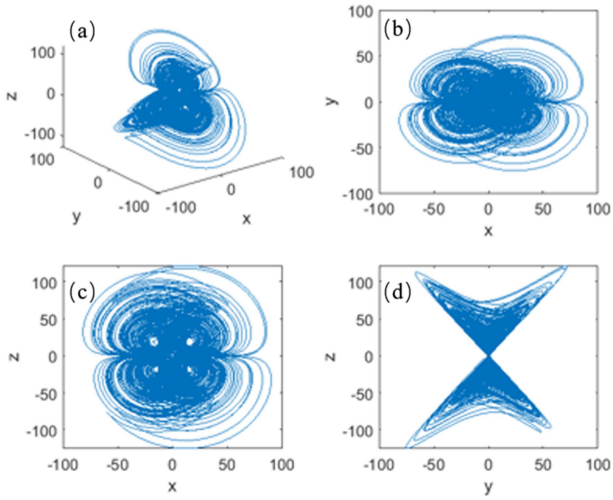

Fig. 4. Hyperchaotic attractors of the Zhan four-wing hyperchaotic system. (a) Projection in x-y-z. (b) Projection in x-y. (c) x-z projection. (d) y-z projection.

further improved through the use of higher order phase modulation [22]. As shown in Fig. 3, Gaussian beams are modulated by adding spiral phase conversion to OAM beams through a spatial optical phase modulator, and as they propagate, the intensity of these OAM beams takes on a 'doughnut' shape in the CCD detection plane, consisting of a bright circle with no intensity in the centre. modulator, which can be converted back to a planar phase front by removing the azimuthal phase term exp (iℓu) from the OAM beam using a spiral phase mask with the opposite end of the modulation. This beam has a bright high intensity point in the centre and finally the original Gaussian beam is restored by means of spatial filtering.

B. 16QAM-OFDM-OAM Encryption Scheme

The bit stream, subcarrier, symbol, and constellation angle in the encryption scheme are disturbed by the Zhan four-wing hyperchaotic system. The equations of the chaos model are as follows (2)

$$\begin{cases} \dot{x} = ax + byz \\ \dot{y} = cy + dxz \\ \dot{z} = exy + kz + mxw \\ \dot{w} = ny \end{cases} \tag{2}$$

where x, y and z are state variables, a, b, c, d, e, k, m and n are system parameters and w is the system state feedback controller. When a = 8, b = −1, c = −40, d = 1, e = 2, k = −14, m = 1 and n = −2, the system can become hyperchaotic and has four wing properties. Also, the Lyapunov exponent is an important parameter to describe the sensitivity of chaotic systems to initial values. A positive Lyapunov exponent means that even if the initial values of two orbits differ by a very small amount, the differences separate exponentially over time, making the system locally unstable and globally stable. The dynamic behaviour of the four-wing hyperchaotic system is more complex and lends itself to data encryption processing. Fig. 4 shows the

hyperchaotic attractors for the initial conditions (0.1, 0.1, 0.1 and 0.1). It can be seen that the phase diagram of the Zhan four-wing hyperchaotic model shows complex chaotic trajectories and bifurcation dynamics. Due to the sensitivity of the initial values of the hyperchaotic model, when the initial value of chaos changes slightly, it will produce almost completely different complex chaotic trajectories.

When a signal encrypted by these complex chaotic trajectories (chaotic sequences) is received, decryption can only be accomplished by having the exact initial value (private key), thus ensuring high security performance. Around the four chaotic sequences X, Y, Z and W generated by the Zhan four-wing hyperchaotic model (as shown in Fig. 1, X, Y, Z and W are vectors consisting of the Zhan four-wing hyperchaotic model variables x, y, z and w, of length M after M iterations at approximately time t), the four chaotic sequences are processed to generate masking factors A, B, C and D, which are used to encrypt bitstream XOR, constellation point rotation, subcarrier permutation and symbol permutation in the frequency domain. The specific rules are as follows.

$$\left\{\begin{array}{c} \mathrm{A} = \mathrm{mod}\left(\mathrm{floor}\left(\mathrm{X}\cdot 10^{10}\right),2\right) \\ \mathrm{B} = \mathrm{round}\left(\left(\mathrm{Y}-\mathrm{fix}\left(\mathrm{Y}\right)\right)\times 180\right)\times\frac{\pi}{180} \\ \mathrm{C} = \mathrm{Tra}\left(\mathrm{mod}\left(\mathrm{Z}\cdot 10^{10},1\right)\times\left(\frac{1}{\mathrm{sort}(Z)}\right)^{T}\right) \\ \mathrm{D} = \mathrm{Tra}\left(\mathrm{mod}\left(\mathrm{W}\times 10^{10},1\right)\times\left(\frac{1}{\mathrm{sort}(W)}\right)^{T}\right) \end{array}\right\} \quad (3)$$

$$\mathrm{baseband\_out\_bits} = \mathrm{bitxor}\left(\mathrm{baseband\_out},\mathrm{A}\right) \quad (4)$$

As shown in (3), this is the masking factor generation rule, where mod is the remainder operation function, round is the rounding function, fix is the rounding to zero function, Tra is the transpose transformation algorithm, sort is the sorting function from smallest to largest, and the superscript T is the symbol for matrix transpose. The transform matrix A (masking factor) of the chaotic sequence X can be obtained by the operation in (3). To ensure the randomness of the sequence, the ten decimal places of the chaotic sequence X are taken for data processing, and then the rounding and pairwise 2 remainder operations are performed to generate a sequence of 0 to 1 integers of the same length as the initial bit stream, which is heterogeneously encrypted with the original data (as shown in process a in Fig. 1). Baseband_out is the initial bit stream, bitxor is the XOR algorithm, and baseband_out_bits is the data after heterogeneous processing of the transformation matrix A of the chaotic sequence X with the initial bits. The decryption effect is not achieved.

The rotation transformation matrix B (masking factor) of the chaotic sequence Y can be obtained by the operation of (3). The chaotic sequence Y is rounded and expanded to obtain a sequence of radians B in the interval $[-\pi, \pi]$ as the constellation point rotation encryption masking factor, which can be added to the phase angle of each constellation point to complete the rotation encryption of the constellation point (as shown in process b in Fig. 1).

$$\mathrm{complex\_carrier\_matrix} = \mathrm{complex\_carrier\_matrix}(:,\mathrm{C}) \quad (5)$$

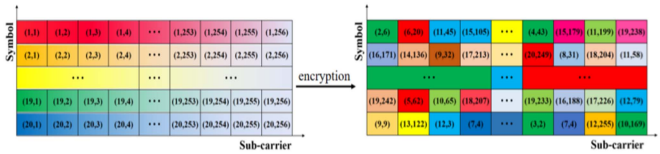

Fig. 5. Effect of OFDM symbol and subcarrier transpose transformation matrix.

$$\mathrm{complex\_carrier\_matrix} = \mathrm{complex\_carrier\_matrix}\left(\mathrm{D},:\right) \quad (6)$$

The transpose transformation matrix C (masking factor) of the chaotic sequence Z can be obtained by the operations of (3) and (5), which are essentially constant matrices that have undergone multiple primary transformations. Subcarrier sub-stitution in the frequency domain can be accomplished by multiplying the transpose transform matrix C with the con-stellation point matrix (as shown by process c in Fig. 1). The transpose transform matrix D is generated in the same way as C and multiplied by the IFFT matrix to complete the symbol substitution (as shown in process d in Fig. 1). The effect of the subcarrier and symbol transpose transform is shown in Fig. 5.

Our chaos model is highly sensitive to initial values. Even if the parameters and initial values of the chaos model change very little at the illegal receiver side, it is still very difficult to decipher.

III. Experimental Setup and Results

The experimental setup is shown in Fig. 6. The data is modulated by the DSP and the signal is sent to an arbitrary waveform generator (Tektronix, AWG70002A) with a sampling rate of 25Gs/s to generate the corresponding electrical waveform which drives the Mach-Zehnder modulator (MZM). A continuous wave (CW) laser operating at 1550 nm with an optical power of 15 dBm is used as the light source, which is fed into the MZM for intensity modulation and then passed through an erbium-doped laser amplifier (EDFA) for optical amplification. It is then injected into the free-space optical system for transmission. In this part of the optical link, the coaxially superimposed beam is reflected by the beam splitter (BS1) and sent to SLM1, which is loaded with a spiral phase pattern for modulation and then the beam is reflected back to BS1 and sent to SLM1, which is loaded with a spiral phase pattern for modulation and then the beam is reflected back to BS1 and transmitted to a second beam splitter prism (BS2). The beam is then transmitted through the coaxial superposition and sent by the beam splitter (BS2) to SLM2, which is loaded with an opposite topological hologram with a helical phase pattern for demodulation. The demo-dulated beam is reflected through a prism into the collimator and the demodulated beam is reflected through a prism into the collimator. At the receiver, the received signal light is amplified using an EDFA, and a variable optical attenuator (VOA) is used to regulate the received optical power. The received optical signal is detected by a 40 GHz photodiode (PD). The detected signal is also sampled

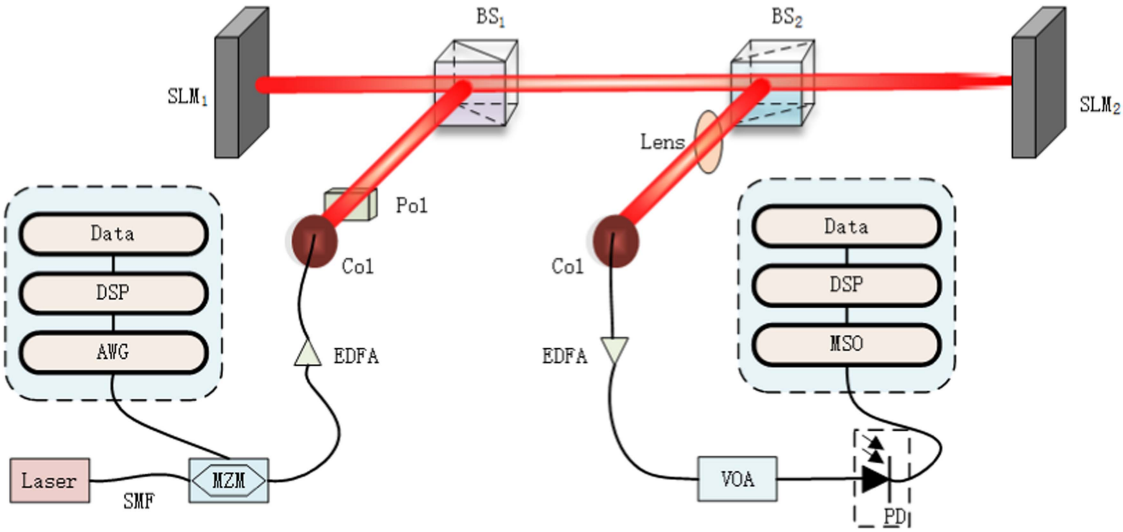

Fig. 6. Experimental setup (AWG: Arbitrary waveform generator; SMF: Single-mode fibre; MZM: Mach-Zendel modulator; EDFA: Optical amplifier; Col: Collimator; Pol: Polariser; BS: Beam splitter; SLM: Spatial light modulator; lens: Lens; VOA: Variable optical attenuator; PD: Photodiode; MSO: Mixed-signal oscilloscope).

using a mixed signal oscilloscope (Tektronix, MSO73304DX) for further digital signal processing.

To improve the accuracy of the experiments, we first tested the performance of the proposed OAM high-security system for single-mode transmission without phase modulator modulation in the BTB case, and then experimentally tested the performance when transmitting unencrypted OFDM signals and encrypted OFDM signals. Finally, the effect of different transmission rates on the encrypted system is investigated.

To investigate the effect of the proposed encryption method on OFDM signals and the effect of the high security OAM modulation system used on OFDM signal trans-mission, encrypted OFDM signals as well as unencrypted OFDM signals were transmitted at a transmission rate of 10 Gbs/s based on a back-to-back system,and the BER curves are reflected in Fig. 7, where the other 0-mode curve shows the BER curve of an OFDM signal without a phase modulator for The BER curve of the OFDM signal without phase modulation and the illegal ONU curve represents the BER curve of the illegal eavesdropper in the case of eavesdropping or violent decryption. Taking into account the experimental error, it can be concluded that the BER generated by the encrypted OFDM signal has almost no effect compared to the unencrypted OFDM signal. The difference between the bit error rate of the high security OAM modulation system within the FEC threshold and the bit error rate of the BTB transmission is small, which confirms the feasibility of the proposed system and is conducive to the subsequent research on OAM multiplexing. At the illegal ONU end, the BER value received by forced decryption is 0.49, which confirms the security of the proposed encryption scheme.

Fig. 8 shows the BER profiles of encrypted OFDM signals modulated and demodulated by phase modulators of different orders at different transmission rates of 10 Gbs/s. Among them, Fig. 8(a) shows the BER profiles for even-order OAM phase

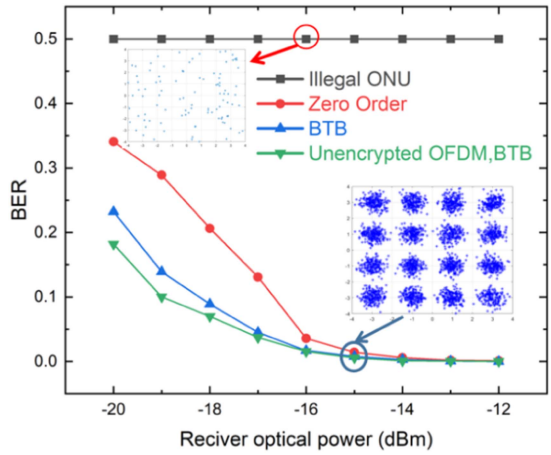

Fig. 7. BER curves for unencrypted OFDM signal in BTB mode, encrypted OFDM signal, 0th order phase modulation in OAM mode and illegal eavesdropper.

modulation. Fig. 8(b) shows the BER profiles for odd-order OAM phase modulation, from which it can be seen that as the modulation order of the phase modulator increases, the BER curve for different modulation orders is relatively close within the FEC threshold, and the BER variation is small and within the controllable range of the system.

Fig. 9 depicts the BER curves at 1 Gbs/s, 5 Gbs/s and 10 Gbs/s. The most representative 6th order and 7th order phase plates were selected for high order OAM modulation to test the transmission performance of the system at different transmission rates, and the test results show that there is less loss in BER immunity as the transmission rate increases.

In addition, the key space of the proposed encryption scheme was rigorously calculated. As shown in Fig. 10, the key consists

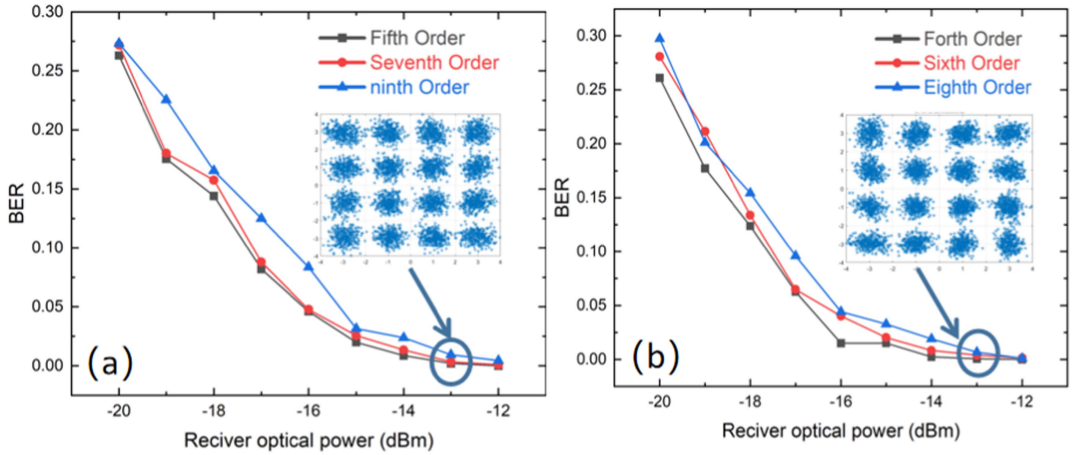

Fig. 8. (a) BER curve for odd-order phase modulation at 10 Gs/s rate. (b) BER curve for even-order phase modulation at 10 Gs/s rate.

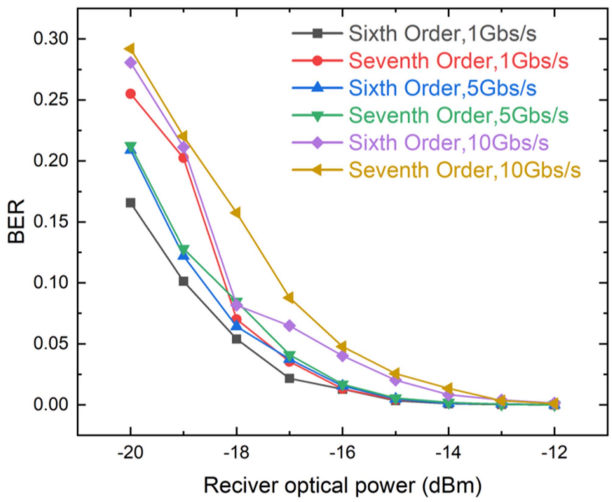

Fig. 9. BER curves for 6th and 7th order phase modulation at different transmission rates.

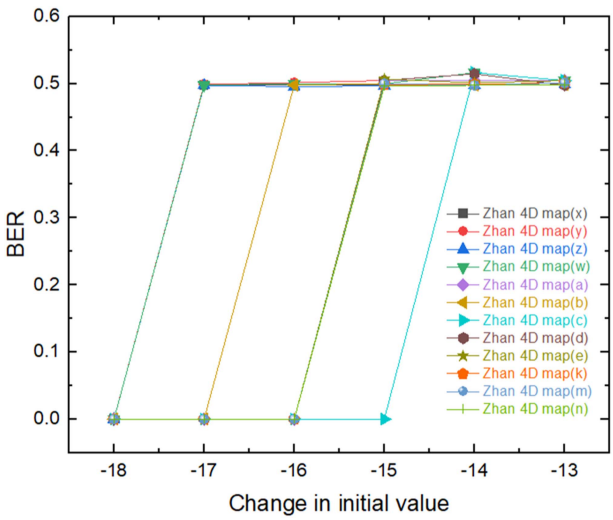

Fig. 10. Sensitivity diagram for chaotic encryption.

of the initial values of the Zhan four-wing hyperchaotic system, the control parameters and the step size {x, y, z, w, a, b, c, d, e, k, m, n, λ}. If the step size is [1, 10^3], Through the sensitivity test experiment, the key space can be strictly calculated by adding 1×10^{-N} to a single initial value or initial parameter, and then experiment to test whether the correct data can be demodulated success-fully. Adjust the size of N until the node with a high bit error rate and an order of magnitude difference from the complete demodulation is the key space. The key space can be experimentally calculated as $10^{17} \times 10^{17} \times 10^{17} \times 10^{17} \times 10^{15} \times 10^{16} \times 10^{14} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{3} = 10^{191}$. Since the key space is so large, it takes a long time even to find the correct key, thus effectively preventing hijackers from obtaining the key.

IV. Conclusion

In this work, we propose a high-security hyperchaotic OFDM encryption scheme based on the orbital angular momentum system. To improve the security of the trans-mission system, the Zhan's hyperchaotic model is used to encrypt OFDM signals and apply it to OAM system trans-mission. In order to verify the possibility of our proposed scheme, we built an OAM optical transmission platform and tested the BER performance of high-order OAM spatial optical modulation. The experimental results show that our proposed encryption scheme has less impact on the bit error rate performance compared with the traditional OFDM signal within the FEC threshold, and compared with the traditional chaotic encryption scheme, we have 10^{191} large key space, which can effectively prevent eavesdroppers from decrypting violently. It is proved that the proposed encryption scheme is a promising candidate for the next generation of high security OAM high order multiplexing transmission system.

References

[1] P. J. Winzer and D. T. Neilson, "From scaling disparities to integrated parallelism: A decathlon for a decade," *J. Lightw. Technol.*, vol. 35, no. 6, pp. 1099–1115, Mar. 2017.

[2] O. Edfors and A. J. Johansson, "Is orbital angular momentum (OAM) based radio communication an unexploited area?," *IEEE Trans. Antennas Propag.*, vol. 60, no. 2, pp. 1126–1131, Feb. 2012.
[3] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, "Orbital angular momentum of light and the transformation of Laguerre—Gaussian laser modes," *Phys. Rev. A Gen. Phys.*, vol. 45, no. 11, pp. 8185, Jun. 1992.
[4] B. Thidé et al., "Utilization of photon orbital angular momentum in the low-frequency radio domain," *Phys. Rev. Lett.*, vol. 99, no. 8, 2007, Art. no. 087701.
[5] F. Tamburini et al., "Encoding many channels on the same frequency through radio vorticity: First experimental test," *New J. Phys.*, vol. 14, no. 4, 2012, Art. no. 033001.
[6] J. Wang et al., "Terabit free-space data transmission employing orbital angular momentum multiplexing," *Nature Photon.*, vol. 6, pp. 488–96, Jun. 2012.
[7] H. Song et al., "Simultaneous turbulence mitigation and mode demultiplexing using one MPLC in a two-mode 200-Gbit/s free-space OAM-multiplexed link," in *Proc. Opt. Fiber Commun. Conf.*, 2020, pp. 1–3.
[8] A. Argyris et al., "Chaos-on-a-chip secures data transmission in optical fiber links," *Opt. Exp.*, vol. 18, no. 6, pp. 5188–5198, 2010.
[9] A. Sultan, X. Yang, A. A. E. Hajomer, S. B. Hussain, and W. Hu, "Dynamic QAM mapping for physical-layer security using digital chaos," *IEEE Access*, vol. 6, pp. 47199–47205, 2018.
[10] A. A. E. Hajomer, X. Yang, and W. Hu, "Chaotic Walsh–Hadamard transform for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 6, pp. 527–530, Mar. 2017.
[11] W. Zhang, C. Zhang, W. Jin, C. Chen, N. Jiang, and K. Qiu, "Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON," *IEEE Photon. Technol. Lett.*, vol. 26, no. 19, pp. 1964–1967, Oct. 2014.
[12] C. Zhang et al., "Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding," *J. Lightw. Technol.*, vol. 36, no. 9, pp. 1706–1712, May 2018.
[13] W. Zhang, C. Zhang, C. Chen, H. Zhang, and K. Qiu, "Brownian motion encryption for physical-layer security improvement in CO-OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 12, pp. 1023–1026, Jun. 2017.
[14] B. Liu et al., "Constellation-masked secure communication technique for OFDM-PON," *Opt. Exp.*, vol. 20, no. 22, pp. 25161–25168, 2012.
[15] Q. Chen et al., "Security scheme in IMDD-OFDM-PON system with the chaotic pilot interval and scrambling," *Opt. Commun.*, vol. 407, pp. 285–289, 2018.
[16] 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.
[17] Z. Zhang et al., "Constellation shaping chaotic encryption scheme with controllable statistical distribution for OFDM-PON," *J. Lightw. Technol.*, vol. 40, no. 1, pp. 14–23, Jan. 2022.
[18] K. Zhan and W. Jiang, "Novel four-wing hyper-chaos system and its application in image encryption," *Comput. Eng. Appl.*, vol. 53, no. 12, pp. 36–44, 2017.
[19] W. Shao et al., "Free-space optical communication with perfect optical vortex beams multiplexing," *Opt. Commun.*, vol. 427, pp. 545–550, 2018.
[20] C. Kai et al., "The performances of different OAM encoding systems," *Opt. Commun.*, vol. 430, pp. 151–157, 2019.
[21] Y. Lian, Y. Yu, S. Han, N. Luan, Y. Wang, and Z. Lu, "OAM beams generation technology in optical fiber: A review," *IEEE Sensors J.*, vol. 22, no. 6, pp. 3828–3843, Mar. 2022.
[22] X. Liu et al., "1.12-Tb/s 32-QAM-OFDM superchannel with 8.6-b/s/Hz intrachannel spectral efficiency and space-division multiplexed transmission with 60-b/s/Hz aggregate spectral efficiency," *Opt. Exp.*, vol. 19, no. 26, pp. B958–B964, 2011.