Security Enhancement in Coherent OFDM Optical Transmission with Chaotic Three-Dimensional Constellation Scrambling

Yiqun Zhang, Ning Jiang, *Senior Member, IEEE*, Anke Zhao, Shiqin Liu, Jiafa Peng, Lu Chen, Martin P. J. Lavery, Hasan Abbas, and Kun Qiu

***Abstract*—In this paper, we propose and experimentally demonstrate a novel hybrid chaos-based three-dimensional (3-D) constellation scrambling scheme to simultaneously improve the physical layer security and transmission performance of the coherent optical orthogonal frequency division multiplexing (CO-OFDM) system. A 3-D regular hexahedron signal constellation is constructed by the constellation figure of merit principle, which not only expands the encryption dimension but improves the error performance. The dynamic parameters for constellation scrambling are generated by the 5-D hybrid chaotic scheme based on the combination of a 3-D hyperchaotic Hénon mapping and two independent 1-D Logistic mappings, as such a key space of ~10^{133} is introduced to enhance the security level of OFDM data encryption during transmission. Furthermore, a transmission experiment for encryption of 144 Gbps 16-quadrature-amplitude-modulation OFDM data over a 100 km standard single-mode fiber in a CO-OFDM system is demonstrated. Compared with the case of using the 3-D rectangular constellation, a 2 dB bit error rate performance improvement is achieved. The results show that the proposed scheme could effectively enhance the system security and transmission performance, which suggests a scalable strategy for future physically secured CO-OFDM systems.**

***Index Terms*—Chaos encryption, orthogonal frequency division multiplexing (OFDM), constellation scrambling, physical layer security.**

I. Introduction

Orthogonal frequency division multiplexing (OFDM) has ignited a great deal of research interest due to its high spectral efficiency, flexible modulation format, and strong robustness against dispersion [1]-[3]. The coherent optical communication system can simultaneously achieve high spectral efficiency, large capacity, and long-haul transmission, in virtue of the combination of high order modulation format, coherent detection technology, and digital signal processing (DSP) technology. However, the majority of the previously-reported studies on coherent optical OFDM (CO-OFDM) systems are focused on the transmission capacity and the optimization algorithms for transmission performance, while the security of the OFDM transmission system is rarely considered. However, due to the openness and fitness of fiber networks, the transmitted data over public fiber is easily accessed by malicious attacks, as such the information security is vulnerable. Traditionally, the security enhancement techniques in optical networks are based on the cryptographic encryption for the data at the media access control (MAC) layer or higher layers. However, this type of encryption cannot protect the header information or control data and has rather complex key management as the number of users increases [4], [5]. Moreover, the conventional cryptographic methods are limited by the processing speed of electronic devices, and then the security is threatened by the superfast computation, such as the emerging quantum computation, which may crack the ciphers in a short time [6]. In contrast, the physical layer can be regarded as a transparent channel for data communication. Therefore, it is valuable to prevent the data transmitted at the physical layer of optical fiber communication systems from being accessed by eavesdroppers.

In recent years, a few physical-layer security enhancement approaches for OFDM transmission systems have been proposed. These approaches can be classified into the optical and electric domain encryptions. Regarding the optical domain encryption, the optical chaos-based communication in virtue of the synchronization of optical chaotic systems can effectively improve the privacy and security of data signals [7]-[10], but there are still some drawbacks. In practical applications, the limited bandwidth and complexity of chaotic carriers would restrict the transmission capacity, and then it cannot be compatible with the present high-speed optical transmission system, such as the coherent communication systems that afford ultra-large capacity and ultra-long-haul transmission ability. On the other hand, for the electric domain encryption, by making use of the convenient digital processing of OFDM signals, the physical layer security enhancement based on DSP has the

This work was supported by the Sichuan Province Science and Technology Support Program (2021JDJQ0023), the National Natural Science Foundation of China under Grant 62171087 and 61671119, the STCSM (SKLSFO2020-05), the Fundamental Research Funds for Central Universities under Grant ZYGX2019J003, and the Exchange Project for Key Lab of Optical Fiber Sensing and Communications (Ministry of Education of China) (ZYGX2021K010). (*Corresponding author: Ning Jiang.*)

Yiqun Zhang, Ning Jiang, Anke Zhao, Shiqin Liu, Jiafa Peng, Lu Chen, and Kun Qiu are with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: uestc_nj@uestc.edu.cn).

Yiqun Zhang is also with the University of Glasgow, Glasgow G12 8LT, U.K. Martin P. J. Lavery and Hasan Abbas are with the University of Glasgow, Glasgow G12 8LT, U.K.

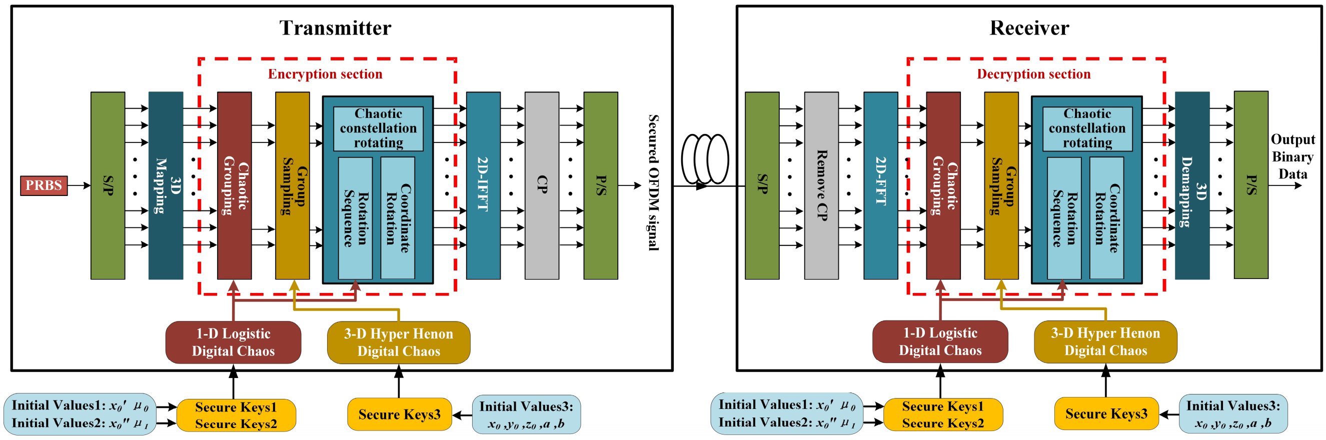
Transmitter
Encryption section
PRBS
S/P
3D Mapping
Chaotic Grouping
Group Sampling
Chaotic constellation rotating
Rotation Sequence
Coordinate Rotation
2D-IFFT
CP
P/S
Secured OFDM signal
1-D Logistic Digital Chaos
3-D Hyper Henon Digital Chaos
Initial Values1: x_0' μ_0
Initial Values2: x_0'' μ_1
Secure Keys1
Secure Keys2
Secure Keys3
Initial Values3: x_0 ,y_0 ,z_0 ,a ,b
Receiver
Decryption section
S/P
Remove CP
2D-FFT
Chaotic Grouping
Group Sampling
Chaotic constellation rotating
Rotation Sequence
Coordinate Rotation
3D Demapping
P/S
Output Binary Data
1-D Logistic Digital Chaos
3-D Hyper Henon Digital Chaos
Initial Values1: x_0' μ_0
Initial Values2: x_0'' μ_1
Secure Keys1
Secure Keys2
Secure Keys3
Initial Values3: x_0 ,y_0 ,z_0 ,a ,b

Fig. 1. Block diagram of the proposed 5-D hybrid hyperchaotic system based three-step constellation scrambling scheme for OFDM signals.

flexibility and feasibility to achieve data encryption without changing any optical module or electrical circuit, which is envisioned as an efficient approach to tackle the security problem of OFDM systems [11]. Digital chaotic encryption has been widely utilized for secure transmission owing to its unpredictability and high sensitivity to initial conditions. Recently, many secure strategies based on digital chaos have been proposed and demonstrated. X. Yang and coworkers proposed to use chaotic precoding [12], [13], and chaotic constellation extension [14] to achieve security enhancement and effective peak to average power ratio (PAPR) reduction. In addition, a physical-layer data encryption scheme using multi-fold chaotic dynamic mapping of 2-D quadrature-amplitude-modulation (QAM) symbols was discussed to reconstruct the random and flexible QAM mapping and provide high-level security [15]. C. Zhang et al. proposed and demonstrated Brownian motion scrambling [16], chaotic constellation transformation with the pilot-aided key agreement [17], and deoxyribonucleic acid (DNA) encoding encryption can all enhance the security of OFDM systems [18]. L. Zhang and B. Liu et al. presented OFDM-PON physical layer security enhancement techniques based on chaos scrambling at the symbol-level and bit-level [19]-[23]. L. Deng and colleagues have experimentally verified that fixed-point digital chaos algorithm [24] and chaos with fractional Fourier transform techniques [25] can meet the demands of OFDM-PON for low implementation complexity and high security performance. It is promising to combine digital chaotic encryption with certain fields to obtain higher security and better system performance [26]. Existing research has shown that higher spectrum and energy efficiency could be achieved in 3-D modulation compared with 2-D modulation [27]. Moreover, multi-dimensional space makes constellation encryption transformation more flexible and increases the key space to further improve the security of the system.

In this paper, we propose and demonstrate a novel constellation scrambling scheme for secure CO-OFDM transmission. The coordination and improvement of system security and transmission performance are considered. In the proposed scheme, a novel 3-D regular hexahedron signal constellation is designed based on the constellation figure of merit (CFM) principle to achieve 3-D QAM mapping for the original data, and a 5-D hybrid hyperchaotic system is adopted to generate chaotic sequences $\{cs_1 - cs_5\}$ to control the rotation of the 3-D QAM symbols. We experimentally demonstrated the transmission of a 144 Gb/s encrypted 16QAM coherent OFDM signal over a 100km standard single-mode fiber (SSMF). The results show that system security enhancement and transmission performance improvement are achieved simultaneously in the proposed scheme. This hybrid hyperchaotic encryption combined with 3-D constellation design may open an alternative route in future secure OFDM systems.

II. Principle and Theoretical Model

The block diagram of the proposed three-step 3-D constellation encryption scheme based on the 5-D hybrid hyperchaotic system in CO-OFDM is depicted in Fig. 1. A pseudorandom binary sequence (PRBS) datastream is first mapped to 3-D QAM symbols, via serial-to-parallel conversion (S/P). Subsequently, an encryption based on chaos techniques is performed before inverse fast Fourier transformation (IFFT). This encryption section consists of three steps: chaotic dynamic grouping, group sampling, and constellation rotation. In step 1, all the 3-D QAM symbols are divided into different groups with random element sizes by chaotic sequence $\{cs_1\}$. To ensure that each constellation point could be controlled by chaos, the chaotic sequences $\{cs_2 - cs_4\}$ are sampled in step 2 at random sampling intervals with specific restriction, and then the results are transformed into the chaotic angle vectors by the trigonometric function, which control the rotation of the x, y, z coordinates of constellation points. In step 3, each specific constellation point is rotated three times in the 3-D space according to the coordinate axis rotation order controlled by the other chaotic sequence $\{cs_5\}$. Hence, a 5-D hybrid hyperchaotic system is used to generate five independent chaotic sequences $\{cs_1 - cs_5\}$, which are then used to generate the chaotic angle matrixes and the chaotic rotation order matrixes for signal encryption.

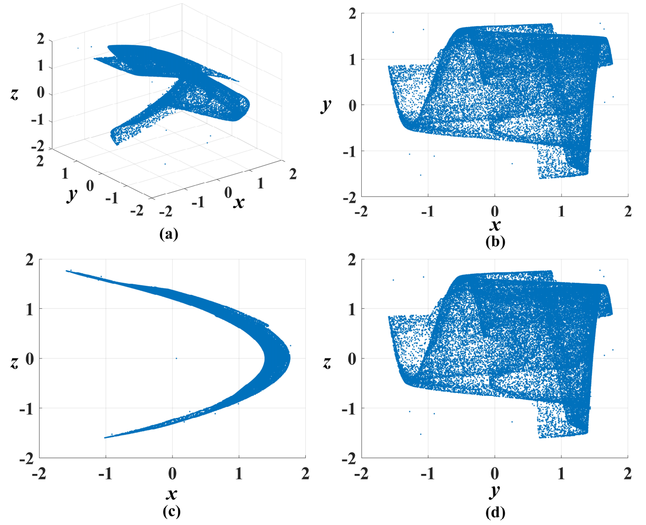

Fig. 2. Phase diagram of the 3-D Hénon hyperchaotic attractor.

A. 5-Dimensional Hybrid Hyperchaotic System

To meet the requirements for the proposed encryption scheme and achieve high security performance, a 5-D hybrid hyperchaotic scheme, with nine independent initial parameters, is applied as the rotation rule to realize the disturbance of the 3-D signal constellation. The chaos-based OFDM uses three chaotic security subsystems (CSSs) that are based on two independent 1-D logistic maps and one 3-D Hénon chaotic system. A 1-D logistic map is employed as the chaos map, defined as [28],

$$x_{n+1} = 1 - \mu x_n^2, \quad x \in [0,1] \,\&\, \mu \in [1,4] \tag{1}$$

where μ is the bifurcation parameter and x_0 is the initial value of the iteration between 0 and 1, and n is the iteration variable. It gets a complex kinetic behavior and changes drastically with the fluctuation of μ in the range of [3.57, 4]. When $\mu = 4$, the logistic map has the largest positive Lyapunov exponent of 0.693.

The 3-D Hénon hyperchaotic system is a three-dimensional quadric autonomous system that can be represented by [29],

$$\begin{cases} x_{n+1} = a - y_n^2 - bz_n \\ y_{n+1} = x_n \\ z_{n+1} = y_n \end{cases} \tag{2}$$

where a and b are control parameters. Generally, with $a \in (1.54, 2)$ and $|b| \in (0, 1)$, this system exhibits hyperchaotic behavior. The initial values of the 3-D Hénon system would be a set of incessant values (x_0, y_0, z_0) chosen within the range [0, 1] for each state output x, y or z [29]. When $a = 1.65$ and $b = 0.15$, the positive Lyapunov exponents of this 3-D hyperchaotic system own the two largest values as, 0.689 and 0.693. The phase diagrams of the chaotic system in various phase planes are illustrated in Fig. 2. It can be seen that a random and unpredictable trajectory is demonstrated in any phase projection, which further verifies its hyperchaotic behavior.

The proposed encryption scheme uses a hybrid of three uncoupled CSSs of degrees 1, 1, and 3. This enables the security enhancement scheme to chaotically control five parameters of the OFDM physical layer. One of the advantages of this hybrid combination is that the correlation of generated chaotic sequences is lower than that of an individual hyperchaotic system with the same dimension. According to this, the hybrid chaotic security system has a higher security level and larger key space compared with the used CSSs. Further, the features of each of the CSS are reserved in the hybrid scheme. In fact, any 3-D and 2-D (or two 1-D) CSSs that can provide five chaotic control sequences, e.g. 3-D modified Duffing chaotic system with 2-D Chen's chaotic system, can be applied to construct this hybrid hyperchaotic scheme. On the other hand, the security performance of a chaos-based system mainly depends on the complex characteristic of the chaotic source, the Lyapunov exponent, which could be used to quantify the sensitivity of the initial value and the complexity of the chaotic system. Each 1-D logistic map CSS has one positive Lyapunov exponent, and the 3-D Hénon hyper-CSS has two positive Lyapunov exponents, so the 5-D hybrid hyperchaotic system employed in this work has a total of four positive Lyapunov coefficients, which means that the outputs of the system will have more complex randomness and higher unpredictability.

B. Three-Step Encryption Scheme for CO-OFDM

Here, we take Chen's 3-D rectangular constellation as an example [30]. The schematic diagram of the three-step physical layer encryption scheme based on hybrid CSSs and constellation scrambling is shown in Fig. 3.

In Step 1 of the proposed encryption scheme i.e., chaotic dynamic grouping, the input bitstream data is mapped into QAM symbols in the 3-D space after serial-parallel conversion. Assuming that the number of constellation points to be encrypted is N, the frequency domain expression of an OFDM symbol can be obtained as,

$$\boldsymbol{S} = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ \vdots & \vdots & \vdots \\ x_N & y_N & z_N \end{pmatrix} \tag{3}$$

where each constellation point is denoted as (x_i, y_i, z_i). The chaotic sequence $\{cs_1\}$ generated by (1) with $\mu_0 = 3.6$ is adopted and quantized as $cs_{1i} \in [-1.5, 1.5]$ to divide the constellation points into different groups with random element sizes. The chaotic dynamic grouping process can be described as,

$$\xi_i = p + floor(q \times cs_{1i}), i = 1, 2, ..., m \tag{4}$$

where m is the number of groups to be determined and ξ_i is the element size (number) of signal points in the i_{th} group. Here we set parameters $p = 29$, $q = 50$ to ensure ξ_i is an integer while satisfying $1 \leq \xi_i \leq N/100$, thereby greatly increasing the degree of disturbance of the transmitted data by chaotic sequences and improving the confidentiality of the encryption scheme. The sum of ξ_i can be written as,

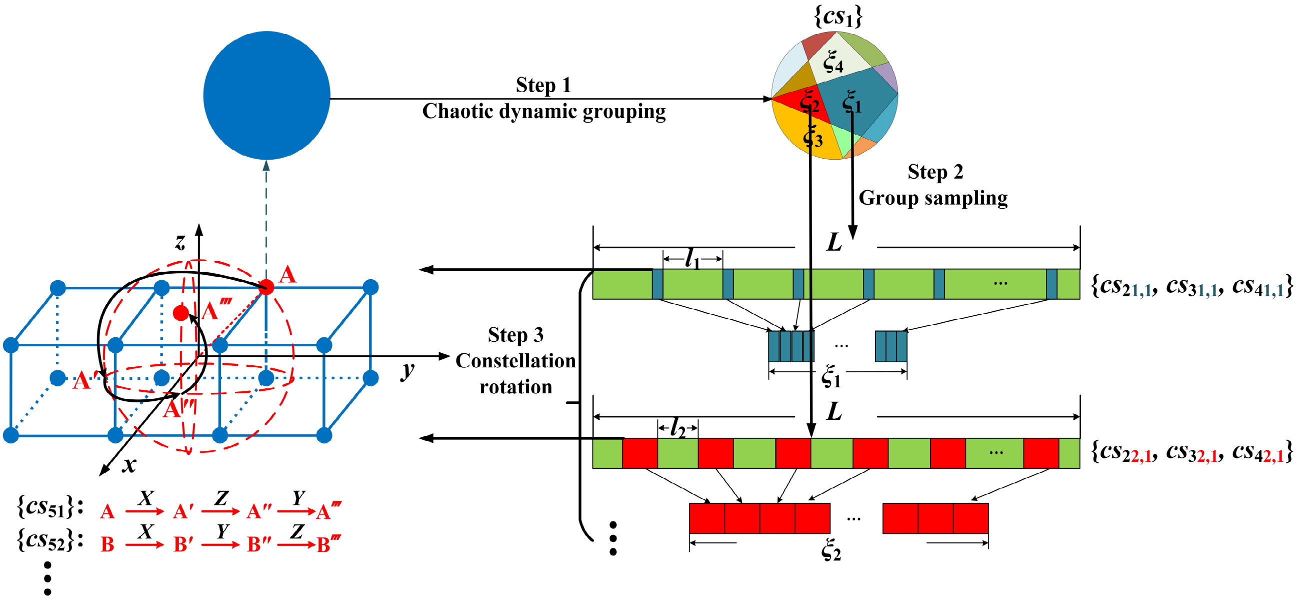

Fig. 3. Schematic diagram of the proposed three-step encryption scheme based on chaos and constellation rotation.

$$\begin{cases} T_m = \sum_{i=1}^{m} \xi_i \\ T_{m-1} = \sum_{i=1}^{m-1} \xi_i \end{cases}. \tag{5}$$

When the conditions $T_{m-1} < N$ and $T_m > N$ are satisfied, only then it can be guaranteed that all 3-D constellation points are divided into groups, without any points missed. The length of the last group can be calculated as,

$$\xi_m = N - \sum_{i=1}^{m-1} \xi_i. \tag{6}$$

The step 2 of the encryption scheme involves group sampling where the original chaotic sequences which originated from (2) are sampled. This is done according to the chaotic grouping sequence ξ_i, and the chaotic sequences $\{cs_2 - cs_4\}$ are then generated that control the three axes of each constellation point to be rotated in step 3. To obtain enough sequences sampled from the original chaotic sequences for encryption, the longest sampling interval f can be written as,

$$f = floor\left(\frac{L}{k}\right) \tag{7}$$

where L is the chaotic iteration length set to 50,000 and k = max(ξ_i). For any group, the sampling interval of the initial chaotic sequences is controlled between $[0, f]$ to ensure that all constellation points can be encrypted. Then the sequence of the group sampling can be expressed as,

$$F = l_i, i = 1,2,3,...,m; 0 \le l_i \le f. \tag{8}$$

Finally, after the first and second levels of encryption, in step 3 of the constellation rotation, based on the grouping size ξ_i and sampling length F, the encryption key for the j_{th} (j=1, 2, 3, …, k) signal point in the i_{th} group can be expressed as,

TABLE I
CORRESPONDENCE BETWEEN BINARY CHAOTIC SEQUENCE AND ROTATION LABEL

Binary cs_{5i}	Rotation label	Rotation order
000	0	x_{axis}→y_{axis}→z_{axis}
001	1	x_{axis}→z_{axis}→y_{axis}
010	2	y_{axis}→x_{axis}→z_{axis}
011	3	y_{axis}→z_{axis}→x_{axis}
100	4	z_{axis}→x_{axis}→y_{axis}
101	5	z_{axis}→y_{axis}→x_{axis}

$$\begin{pmatrix} cs_{2i,j} \\ cs_{3i,j} \\ cs_{4i,j} \end{pmatrix} = \begin{pmatrix} x_{1+(l_i+1)(j-1)} \\ y_{1+(l_i+1)(j-1)} \\ z_{1+(l_i+1)(j-1)} \end{pmatrix}. \tag{9}$$

The chaotic angle vectors can be obtained after transforming $\{cs_2 - cs_4\}$ into rotation angles by,

$$\begin{pmatrix} \theta_{i,j} \\ \varphi_{i,j} \\ \chi_{i,j} \end{pmatrix} = \begin{pmatrix} 180\arctan\left(cs_{2i,j}\right)/\pi \\ 180\arctan\left(cs_{3i,j}\right)/\pi \\ 180\arctan\left(cs_{4i,j}\right)/\pi \end{pmatrix}. \tag{10}$$

Thereafter, the chaotic angle matrixes of the constellation points rotating around the x, y, and z coordinate axes in the 3-D space can be deduced as,

$$\boldsymbol{X} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta_{i,j} & -\sin\theta_{i,j} \\ 0 & \sin\theta_{i,j} & \cos\theta_{i,j} \end{bmatrix} \tag{11}$$

$$\boldsymbol{Y} = \begin{bmatrix} \cos\varphi_{i,j} & 0 & \sin\varphi_{i,j} \\ 0 & 1 & 0 \\ -\sin\varphi_{i,j} & 0 & \cos\varphi_{i,j} \end{bmatrix} \tag{12}$$

$$\boldsymbol{Z}=\begin{bmatrix}\cos\chi_{i,j} & -\sin\chi_{i,j} & 0\\ \sin\chi_{i,j} & \cos\chi_{i,j} & 0\\ 0 & 0 & 1\end{bmatrix}. \tag{13}$$

The chaotic angle matrixes indicate that even if the rotation angle vectors of constellation points are the same, the 3-D coordinates of the final encrypted constellation points will be different due to the different rotation order of the chaotic angle matrixes. Correct decryption can only be achieved by rotating in the reverse order at the receiving end. Therefore, it is reasonable to consider the rotation order as an important factor for the encryption process. Here, another 1-D logistic map is adopted with $\mu_1 = 3.7$ to generate a new chaotic sequence cs_5 to control each point's rotation order, which is quantized as,

$$x_n=\begin{cases}0, x_n\le 0\\ 1, x_n>0\end{cases} \tag{14}$$

and then convert cs_5 to the rotation label according to Table I.

The final position of each constellation point is obtained after chaotic three times rotation encryption controlled by $\{cs_2-cs_5\}$. Each rotation requires a chaotic angle matrix, if it is rotated only once, the constellation point is distributed on a circle that is perpendicular to the rotation matrix. For the 3-D rotation, the distribution of constellation point is on a spherical surface formed by the three rotation matrixes, therefore the security performance is greatly improved. Assuming that the 3-D coordinate of the j^{th} signal point in the i^{th} group to be encrypted is A (x, y, z) shown in Fig. 3, and the rotation order is from x_{axis} → z_{axis} → y_{axis}. The first-time rotation is controlled by the chaotic angle matrix $\boldsymbol{X}$. Point A rotates counterclockwise around the circular curve which is parallel to the yoz plane to reach A′ (x', y', z'). The rotation transformation can be expressed as,

$$\begin{pmatrix}x'\\ y'\\ z'\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\ 0 & \cos\theta_{i,j} & -\sin\theta_{i,j}\\ 0 & \sin\theta_{i,j} & \cos\theta_{i,j}\end{pmatrix}\times\begin{pmatrix}x\\ y\\ z\end{pmatrix}. \tag{15}$$

Then the second-time rotation is controlled by $\boldsymbol{Z}$. Point A′ rotates counterclockwise around the circular curve which is parallel to the xoy plane to reach A″ (x'', y'', z''). The rotation transformation can be expressed as,

$$\begin{pmatrix}x''\\ y''\\ z''\end{pmatrix}=\begin{pmatrix}\cos\chi_{i,j} & -\sin\chi_{i,j} & 0\\ \sin\chi_{i,j} & \cos\chi_{i,j} & 0\\ 0 & 0 & 1\end{pmatrix}\times\begin{pmatrix}x'\\ y'\\ z'\end{pmatrix}. \tag{16}$$

The third-time rotation is controlled by $\boldsymbol{Y}$. Point A″ rotates counterclockwise around the circular curve which is parallel to the xoz plane to reach A‴ (x''', y''', z'''). The rotation transformation can be expressed as,

$$\begin{pmatrix}x'''\\ y'''\\ z'''\end{pmatrix}=\begin{pmatrix}\cos\varphi_{i,j} & 0 & -\sin\varphi_{i,j}\\ 0 & 1 & 0\\ \sin\varphi_{i,j} & 0 & \cos\varphi_{i,j}\end{pmatrix}\times\begin{pmatrix}x''\\ y''\\ z''\end{pmatrix}. \tag{17}$$

Therefore, the encrypted positions of the constellation points are dynamically distributed on a spherical surface with the origin as the center of the sphere and the distance from the origin to the initial position of the constellation point as the radius. The final distribution of all constellation points is the union of these spheres.

All the constellation points $\boldsymbol{S} = (\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_N)^T$ will rotate three times according to (15)-(17). Finally, the obtained encrypted data information is transformed into two channel *I/Q* signals [31],

$$\tilde{\boldsymbol{S}}=\begin{pmatrix}x_1'''+jy_1'''\\ z_1'''+jx_2'''\\ y_2'''+jz_2'''\\ \vdots\\ z_{N-1}'''+jx_N'''\\ y_N'''+jz_N'''\end{pmatrix} \tag{18}$$

which is prepared for the coherent transmission in the experiment, and then transmitted to the receiver end after performing IFFT, cyclic prefixes (CP) addition, and parallel-serial conversion. In this work, we assume that the initial keys of the proposed 5-D hybrid hyperchaotic system at the transmitter and receiver sides are shared in advance, which are defined as double-precision real numbers with 15 decimals in DSP calculations.

C. 3-Dimensional Regular Hexahedron Constellation Design

The signal constellation is one of the essential components to form a digital communication system [30]. To match the requirements of the entire high-dimensional modulation and demodulation system, expanding the traditional 2-D modulation constellation space into the higher dimension can simultaneously improve the overall transmission rate and robustness of the communication system, which has been extensively studied in the fields of wireless communication and optical communication. On the other hand, the high-dimensional constellation can also provide a large dimension space for digital encryption algorithms and further improve the security of the system.

CFM reflects the efficiency of the lattice-based constellations [32]. A constellation with a large CFM means a low symbol error rate. The process of maximizing the CFM of the constellation is constructed as a series of optimization problems, and the geometric characteristics of the constellation are used as constraints of the optimization problems [33]. By solving the optimization problems, the design criteria of the required constellation can be obtained, which can be used as a general method for constructing high-dimensional constellations. The CFM of an n-dimensional constellation $\boldsymbol{C}$ can be expressed as [32],

$$CFM(\boldsymbol{C})=\frac{d_{\min}^2(\boldsymbol{C})}{E_{avg/2D}(\boldsymbol{C})} \tag{19}$$

where $d_{min}(\boldsymbol{C})$ refers to the minimum euclidean distance (MED) between any two constellation points in the constellation $\boldsymbol{C}$, $E_{avg/2D}$ is the defined 2-D average energy, which represents the value of the average power of the n-dimensional constellation converted into 2-D space and can be calculated as,

$$E_{avg/2D}(\boldsymbol{C})=\frac{2}{n}E_{avg}=\frac{2}{nM}\sum_{m\in\boldsymbol{C}}\left\|\boldsymbol{x}_{\boldsymbol{m}}\right\|^2 \tag{20}$$

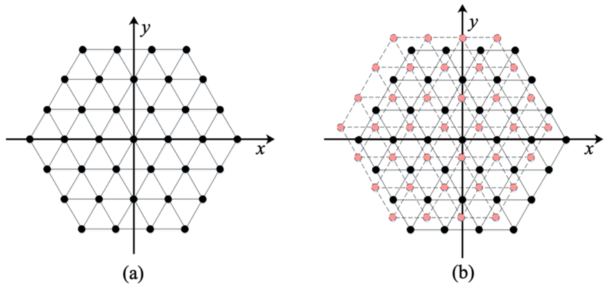

Fig. 4. 3-D lattice structure with G3 as the generator matrix. (a) Single layer points distribution; (b) Top view points distribution.

where M is the number of constellation points in $\boldsymbol{C}$, and $\boldsymbol{x_m}$ is the n-dimensional coordinate vector of the constellation points in $\boldsymbol{C}$. The process of designing a lattice-based constellation includes the selection of lattice and its boundaries. The CFM of $\boldsymbol{C}$ can be decomposed into the basic coding gain of the lattice and the shape gain of the boundary, which can be written as [34],

$$CFM(\boldsymbol{C}) \approx CFM_0 \cdot \gamma_c(\Lambda) \cdot \gamma_s(\Re) \tag{21}$$

where CFM_0 is a constant that is the CFM of the simplest n-dimensional constellation with cubic boundary and can be used as a baseline CFM for comparison with other constellations, $\gamma_c(\Lambda)$ is the coding gain of n-dimensional lattice Λ, $\gamma_s(R)$ is the shape gain of the boundary R. The coding gain $\gamma_c(\Lambda)$ depends on the selection of the lattice. A compact lattice with high coding gain means that more constellation points can be placed in a certain volume and the MED provided by the unit volume is large. On the other hand, the shape gain $\gamma_s(R)$ only depends on the selected boundary of the constellation, and the region R with a high shape gain can improve the power efficiency of the constellation. Equation (21) shows that the CFM of a given constellation can be regarded as the product of two independent terms, $\gamma_c(\Lambda)$ and $\gamma_s(R)$. The maximum value of CFM can be obtained by maximizing $\gamma_c(\Lambda)$ and $\gamma_s(R)$, respectively. These two terms can be described as [34],

$$\gamma_c(\Lambda) = \frac{d^2_{\min}(\Lambda)}{[V(\Lambda)]^{\frac{2}{n}}} = \frac{d^2_{\min}(\Lambda)}{[|\det(\boldsymbol{G})|]^{\frac{2}{n}}} \tag{22}$$

$$\gamma_s(\Re) = \frac{[V(R)]^{\frac{2}{n}}}{6E_{avg/2D}}. \tag{23}$$

$V(\Lambda)$ is the base volume that represents the reciprocal of the number of points in the unit volume of lattice Λ. $\boldsymbol{G}$ is the generator matrix of lattice Λ. $V(R)$ represents the volume of region R. It has been proven that among all possible boundaries in n-dimensional space, the spherical boundary is the most efficient [34]. When n approaches infinity, the spherical boundary can provide the maximum shape gain of $\pi e/6$, which is approximately 1.533 dB. In this work, n is set to 3 to form a three-dimensional constellation, therefore, the primary objective is to select a 3-D lattice with the largest coding gain. Without loss of generality, set the MED d_{min} to 1, and the optimization problem of maximizing $\gamma_c(\Lambda)$ can be described by the following formula [33],

$$\begin{aligned} &\arg_{G(\Lambda)} \ \min|\det(\boldsymbol{G}(\Lambda))| \\ &s.t. \quad d_{\min} = 1. \end{aligned} \tag{24}$$

Reference [33] uses the interior point method to get the solution of this optimization problem, which is,

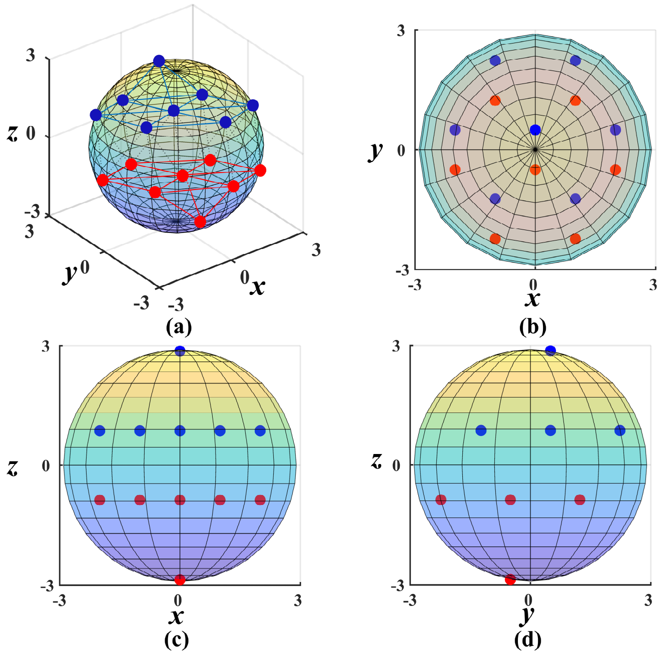

Fig. 5. The new 3-D 16-ary regular hexahedron signal constellation in (a) 3-D space; (b) in x-y projection, (c) in x-z projection; (d) in y-z projection.

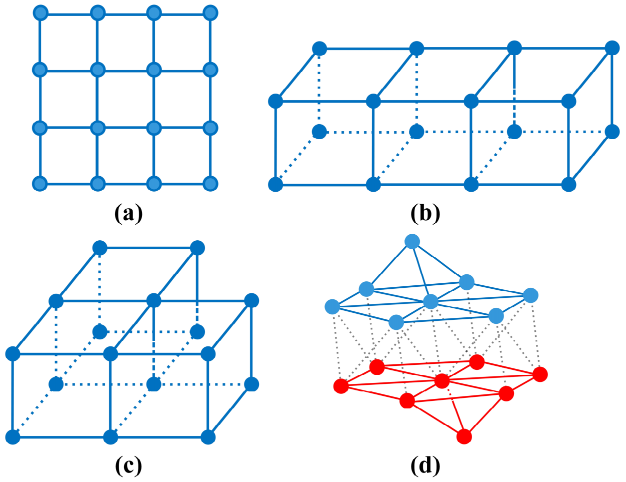

Fig. 6. 16-ary constellations (a) 2-D rectangular constellation; (b) 3-D rectangular constellation; (c) 3-D L-shape constellation; (d) 3-D regular hexahedron constellation.

$$\boldsymbol{G}_3(\Lambda)=\begin{bmatrix}1 & 0 & 0\\ 1/2 & \sqrt{3}/2 & 0\\ 1/2 & \sqrt{3}/6 & \sqrt{6}/3\end{bmatrix}. \tag{25}$$

The maximum coding gain of the 3-D lattice can be calculated as,

$$\gamma_{c\max}=\frac{d_{\min}^2(\Lambda)}{[|\det(\boldsymbol{G})|]^{2/3}}=\frac{1^2}{\left(\frac{\sqrt{2}}{2}\right)^{\frac{2}{3}}}\approx 1.26=1.003\text{dB}. \tag{26}$$

According to the relationship between the basis vectors of $\boldsymbol{G}_3$, the 3-D lattice has a regular hexahedron distribution, and its single layer view and top view of constellation-point distribution are shown in Fig. 4. On the other hand, as mentioned before, the shape gain of the spherical boundary is the largest among all n-dimensional boundaries. According to (23), the shape gain of the 3-D spherical boundary can be calculated as,

$$\gamma_s(\Re)=\frac{[V(R)]^{\frac{2}{3}}}{6E_{avg/2D}}\approx\frac{n[V(R)]^{\frac{5}{3}}}{12\int_{\Re}\|x\|^2\,\mathrm{d}x}=1.083=0.346\text{dB}. \tag{27}$$

From (26) and (27), the $CFM(\Lambda_3)$ of the 3-D constellation based on the baseline CFM with $\boldsymbol{G}_3$ as the generator matrix and sphere as the boundary is $\gamma_c(\Lambda)+\gamma_s(R)=1.349$ dB. Considering $M=2^4=16$, a novel 3-D regular hexahedron 16QAM constellation is designed based on the CFM principle, whose 3-D structure is shown in Fig. 5. The constellation points of this new 3-D constellation satisfy the regular hexahedron lattice distribution on each single layer (blue points in the top layer and red points in the bottom layer), and the basis vectors are also extended into a hexahedron in the 3-D space. Meanwhile, the boundary of the designed 3-D constellation is close to the sphere.

Fig. 6 demonstrates several 16-ary signal constellations, which are 2-D rectangular constellation, Chen's 3-D rectangular and L-shape constellations, and the designed 3-D regular hexahedron constellation. Setting the MED d_{min} to 2, the peak and average power and CFM-related gain coefficients of these constellations are shown in Table II. It can be seen that the peak power and average power of the 3-D constellations are both significantly lower than those of the 2-D constellation. In particular, for the novel regular hexahedron constellation, the average power is reduced by about 53%, more than half. Compared with Chen's two 3-D constellations, the proposed new 3-D constellation not only has the lower average power, but also has significantly improved *CFM* gain. To further verify the inherent characteristic performance of the constellations, the theoretical symbol error probabilities (SEPs) and the Monte Carlo simulation are calculated in the AWGN environment. In addition to the AWGN channel, a uniformly distributed random variable $\boldsymbol{U}$ in (0, 1) is applied to generate the initial binary signal sequence. The SEP of the n-dimensional constellation under the condition that signal-to-noise ratio (SNR) ≥ 8 dB can be expressed as [34],

TABLE II
16-ARY CONSTELLATIONS PERFORMANCE

Constellation	2-D Rectangular 16QAM	3-D Rectangular 16QAM	3-D L-shape 16QAM	3-D Regular hexahedron 16QAM
Peak power	18	11	9	6.7321
Average power	9.9258	7	6.0308	4.6667
Average power drop	0%	30%	40%	53%
Coding gain	1	0	1	1.260
Shape gain	1	0.5673	0.8399	1.083
CFM/*CFM*$_0$	1	0.5673	0.8399	1.365

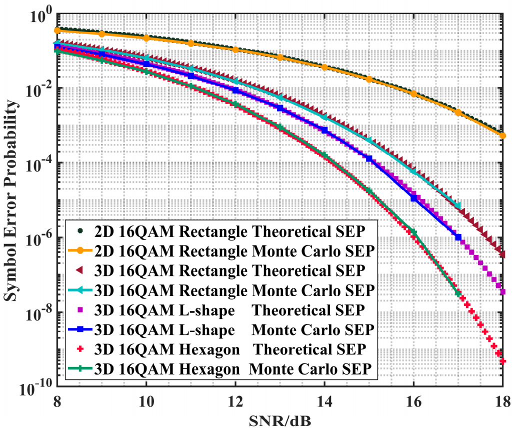

Fig. 7. SEPs of the 16-ary signal constellations.

$$P_e\approx N_{\min}Q\left(\sqrt{\frac{d_{\min}^2}{2E_{avg/2D}}\cdot\frac{E_s}{N_0}}\right) \tag{28}$$

where N_{min} is the number of points in lattice Λ with a distance d_{min} from any given lattice points. $Q(\cdot)$ is the Gaussian Q-function. E_s/N_0 represents SNR. In the proposed scheme, $N_{min}=5$, $d_{min}=2$, $E_{avg/2D}=2E_{avg}/3$, $E_{avg}\approx 4.6667$. Monte Carlo simulation with 5×10^{10} 3-D symbols is carried out to estimate the SEPs of these constellations in the 3-D transmission system according to ref. [35]. The theoretical and simulation results are plotted in Fig. 7. It can be observed that the simulation results of the presented constellations in the AWGN channel match exactly the theoretical SEPs. The SEPs of three 3-D constellations are improved about 3~5 dB as compared with the 2-D constellation at the SEP of 10^{-4}. Compared with the 3-D rectangular constellation and 3-D L-shape constellation, the SEP of the proposed regular hexahedron constellation has an improvement of 1.5 dB and 1 dB, respectively. Such performance gain is attributed to the increased *CFM* of the proposed scheme. It is worth mentioning that to make full use of the advantages of 3-D constellation and realize true 3-D transmission in reality, 3-D modulation and demodulation are necessary. In optical transmission systems, 3-D transmission can be achieved using I/Q modulation in combination with one additional polarization modulator. In wireless transmission systems, high-quality wireless transmission can be achieved by

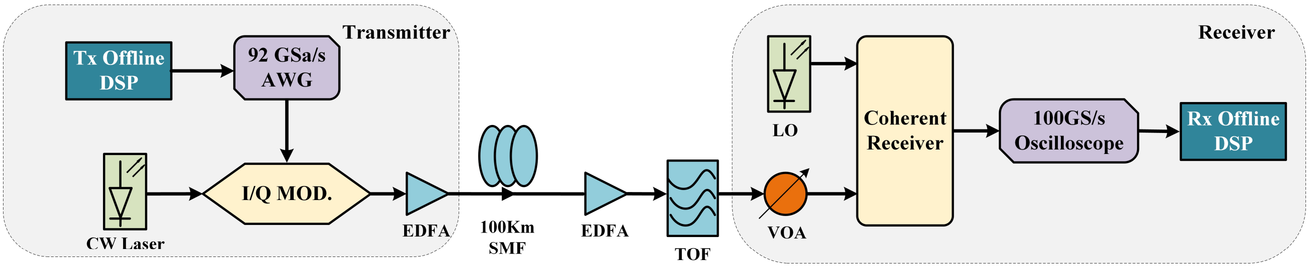

Fig. 8. Experimental setup of the CO-OFDM with proposed three-step QAM scrambling scheme (AWG: arbitrary waveform generator, I/Q MOD: I.Q modulator, EDFA: erbium doped fiber amplifier, SMF: single mode fiber, TOF: tunable optical filter, VOA: variable optical attenuator, LO: local oscillator).

mapping the information into 3-D space and adopting vector antennas as 3-D modulator/demodulator for direct 3-D constellation transmission. However, 2-D optical I/Q modulation (i.e., using a single I/Q modulator) to achieve 3-D transmission would limit the advantages of the 3-D constellation. For instance in ref. [36], a polarization modulator was not used and instead time-division multiplexing was used to attain the additional degree of freedom which for obvious reasons decreases the net data rate.

III. Experimental Setup

Fig. 8 illustrates the experimental setup of the proposed secure CO-OFDM system based on the three-step QAM scrambling. At the transmitter end, the encrypted OFDM datastream is generated through DSP offline. Thereafter, the encrypted signal is used to modulate a CW laser through an I/Q modulator and then transmitted over a 100km optical fiber. At the receiver end, coherent detection of the received signal and demodulation of OFDM symbols are implemented. Finally, the original data is recovered after DSP and decryption operations.

In the off-line DSP, the original PRBS datastream with a length of 2^{15}-1 is first mapped into 3-D 16QAM data symbols. An IFFT/FFT size of the original OFDM signal is 128. The pilot tones are inserted every 32 subcarriers. Subsequently, CP and guard interval of 1/16 OFDM symbol length are inserted into the time domain signal, which is appended to prevent inter-symbol interference (ISI) after performing IFFT of the encrypted data and P/S conversion. Thereafter, the encrypted OFDM signal is loaded into an arbitrary waveform generator (AWG) with a sampling rate of 45 GSa/s to generate the corresponding electrical signal waveform. The net data rate of the transmitted OFDM signals is approximately 144 Gb/s. The encrypted signal from the AWG is used to modulate a CW light at 1550 nm through an optical IQ modulator. Subsequently, after amplified using an Er-doped fiber amplifier (EDFA), the optical signal having a power of 6 dBm is transmitted through a 100km SSMF with a total attenuation of 22 dB.

At the receiver end, a variable optical attenuator (VOA) is employed to emulate different received optical power (ROP) values. Then the optical signal is coherently detected using a local laser in a coherent receiver module. The linewidth of the local laser is less than 100 kHz and the frequency offset is about 300 kHz. After coherent detection, the received optical signal is converted into an electrical signal and then digitized by a digital phosphor oscilloscope (DPO) at the sampling rate of 100 GSa/s. Following the analog-to-digital conversion, the sampled signals are processed through offline DSP that helps analyze the system performance. The offline DSP operation at the receiver end is followed as: 1) IQ imbalance compensation; 2) chromatic dispersion compensation; 3) frequency offset estimation; 4) resample and frame synchronization; 5) match filter and down sampling; 6) carrier phase recovery; 7) channel estimation and equalization; 8) QAM symbols decryption and demapping; 9) BER decision.

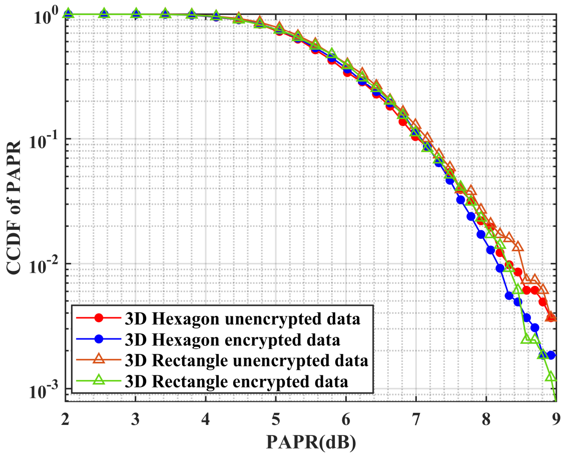

Fig. 9. CCDF of PAPR for different OFDM signals.

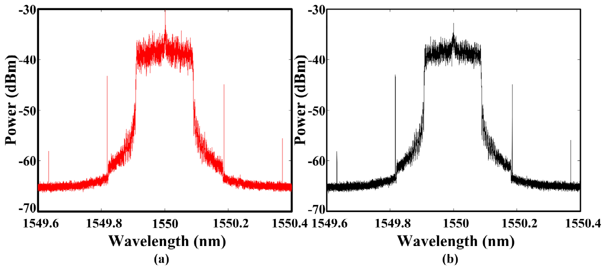

Fig. 10. Optical spectra of OFDM signals after fiber transmission (a) without encryption (b) encrypted with the proposed scheme.

TABLE III

LATENCY OF PROPOSED METHOD WITH DIFFERENT BIT LENGTH

Bitstream length	2^{13}-1	2^{14}-1	2^{15}-1	2^{16}-1
Encryption time	0.654s	0.632s	0.642s	0.630s
Total time (sender)	6.423s	6.190s	6.267s	6.144s
Time proportion (sender)	10.18%	10.22%	10.24%	10.26%
Decryption time	0.513s	0.510s	0.499s	0.529s
Total time (receiver)	44.487s	43.655s	43.073s	45.296s
Time proportion (receiver)	1.15%	1.17%	1.16%	1.17%

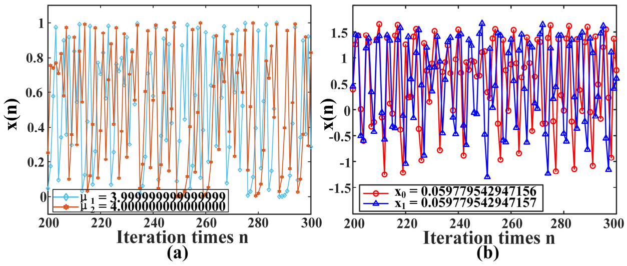

Fig. 11. Sensitivity of the designed 5-D hybrid hyperchaotic system in the case of $x(n)$ slightly different initial condition: (a) $\Delta\mu = 10^{-15}$ in logistic map; (b) $\Delta x_0 = 10^{-15}$ in 3-D Hénon map.

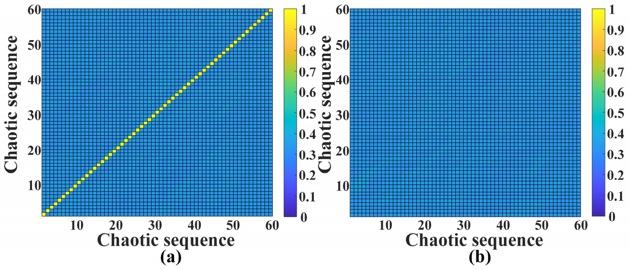

Fig. 12. Correlation coefficients of chaotic sequence {cs_2} (a) with the correct security key; (b) with the wrong security key ($\Delta x_0 = 10^{-15}$).

IV. RESULTS AND DISCUSSIONS

A. PAPR and Optical Spectrum Analysis

Fig. 9 demonstrates the complementary cumulative distribution function (CCDF) of the PAPR of the encrypted and unencrypted CO-OFDM signals with different constellations. It can be seen that the PAPR of both unencrypted and encrypted signals are virtually the same, which indicates the proposed three-step encryption scheme does not bring any PAPR deterioration compared with the original signals. On the other hand, the encrypted OFDM signals using the proposed 3-D regular hexahedron constellation and Chen's 3-D rectangular constellation have similar CCDF curves, which shows that the selection of 3-D constellations will not improve the nonlinearity tolerance of the OFDM system significantly.

In Fig. 10, we present the comparison of the optical spectrum between the original unencrypted OFDM signal and the encrypted OFDM signal after fiber transmission. The results show that, the optical spectrum is hardly affected by the 5-D chaotic encryption algorithm and there is no significant difference observed by comparing these two spectra. It is speculated that the harmonics in the optical spectra are caused by the AWG reference frequency doubling phenomenon due to the nonlinear effect of the AWG device during operation.

B. Latency Analysis

At present, the physical layer security improvement technology of the OFDM signal using the digital chaotic system combined with DSP is still in the frontier exploration stage. Most encryption schemes employ MATLAB-based offline DSP processing, with less consideration of latency, therefore research in real-time systems is still rare. In this work, a personal computer (PC) with 8-GB memory, Intel core$^{\text{TM}}$ i5-10210U and Windows 11 system is used to test the time required for the encryption and decryption process to analyze the latency effect of the proposed method. The results are shown in Table III, in which we can see that the encryption process takes about 0.6s and the decryption process takes about 0.5s, accounting for about 10% and 1% of the total time at the sender and receiver ends, respectively. Multiple coherent detection algorithms take up most of the time at the receiver. Therefore, the additional latency introduced by our encryption and decryption scheme has little effect on the entire OFDM system.

In addition, the real-time end-to-end transmission of an FPGA-based OFDM signal was successfully achieved in ref. [37]. The three-step chaotic constellation rotation encryption is actually an algorithm based on matrix operations, therefore, in virtue of mature FPGA and DSP technology, the proposed scheme can be implemented in real-time applications.

C. Security Performance

The security of the proposed encryption scheme can be evaluated via the sensitivity of digital chaotic sequences to the chaotic initial values. Fig. 11 illustrates the sensitivity of the 5-D hybrid hyperchaotic system in the case of generated $x(n)$. A tiny difference of x_0 is introduced, which is equal to 10^{-15}, in cases (a) and (b). It can be clearly seen that an ultra-small change in the initial conditions would result in completely different iteration trajectories in the logistic map and 3-D Hénon hyperchaotic system, which indicates that the hybrid chaotic system is extremely sensitive to initial values. The size of the key space directly affects whether the system can effectively prevent eavesdropper attacks. The security keys of this encryption system consist of the initial conditions and parameters of the designed 5-D hybrid hyperchaotic systems, which can be written as $\{a, b, x_0, y_0, z_0, x_0', x_0'', \mu_0, \mu_1\}$. The key space provided by the 3-D hyperchaotic Hénon system is $(2-1.54)\times10^{15}\times(1\times10^{15})^4 = 4.6\times10^{74}$. The two independent 1-D Logistic maps can provide a key space of $((4-3.57)\times10^{15}\times(1\times10^{15}))^2 = 1.849\times10^{59}$. Therefore, the total key space of the designed 5-D hybrid hyperchaotic system can reach a size of approximately 8.5×10^{133}. Such a large key space size can sufficiently resist brute-force attacks from illegal attackers.

Furthermore, the correlation operations of one of the chaotic sequences {cs_2} with and without the security key are also

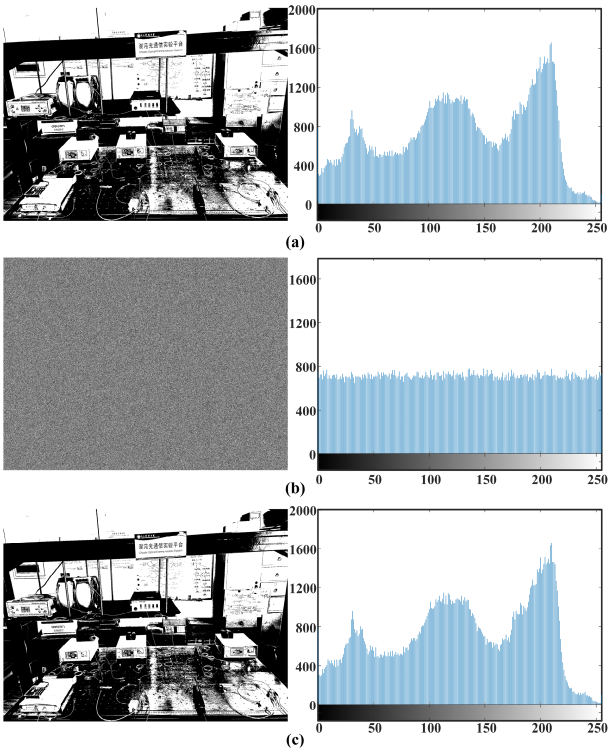

Fig. 13. Images and histograms of (a) the original data, (b) the received data with wrong keys, (c) the received data with exact keys.

investigated. As depicted in Fig. 12 (a) and (b), it can be noticed that only the same chaotic sequence can get the maximum correlation coefficient and no correlation peak when using the wrong security key. Such a result further proves that the eavesdropper cannot recover any useful information by using the wrong security key, which is just slightly different from the correct security key.

To resist statistical analysis attack by an eavesdropper, the encrypted data should have no or very few statistical similarities to the original data. Here we take a picture of our experimental platform which is used as an example to illustrate the ability of the proposed scheme to resist statistical attack. Figure 13(a) presents the original picture and its histogram. Figure 13(b) and (c) show the pictures and histograms at the illegal receiver with wrong keys and the intended receiver with exact keys, respectively. It is observed that the data value distribution of the original data is not uniform, while the data value of the illegal receiver presents a flat and uniform distribution. The eavesdropper barely gets any statistical information, which confirms that the proposed scheme in this paper can effectively resist statistical analysis attacks.

D. BER Performance

Fig. 14(a) presents the BER performance of 144 Gb/s encrypted and unencrypted 16QAM-OFDM signal versus the ROP at the PD. The measured receiver sensitivity at the forward error correction (FEC) limit of the encrypted 16QAM-OFDM signal is -38 dBm in back-to-back (B2B) and -37 dBm after 100 km SSMF transmission, corresponding to a transmission penalty of 1 dB. Moreover, after propagation, the transmission performance of the unencrypted 16QAM-OFDM signal is deteriorated by about 0.5 dB compared with the encrypted case. This could be attributed to the decreased PAPR after the proposed encryption scheme. For the illegal receiver with the wrong key, the BERs are maintained at around 0.4, which greatly exceeds the FEC limit. The received constellations in the positions of A, B in Fig. 14(a) are shown in Fig. 14(b) and (c). A and B represent the correctly decrypted constellation and incorrectly decrypted constellation, respectively. Almost all the constellation symbols are in error at the illegal end, indicating that no useful information from the eavesdropper can be recovered. These results can verify that the proposed scheme has excellent resistance to eavesdropping from any illegal receivers.

In addition, the encrypted OFDM signals with different constellations are investigated. Fig. 15(a) depicts the BER curves of the two OFDM signals with the proposed 3-D regular hexahedron constellation and Chen's 3-D rectangular constellation after 100 km SSMF transmission. The BER of the encrypted 3-D regular hexahedron 16QAM-OFDM signal drops below the FEC limit when ROP is about -37 dBm and -35 dBm for the encrypted 3-D rectangular 16QAM-OFDM signal. There is a 2 dB BER performance improvement when the novel-designed 3-D constellation is applied. This verifies that the novel 3-D constellation based on the CFM principle is well-designed and is more superior in the performance of resisting noise, thus can finally improve the transmission performance of the CO-OFDM system. By comparing the received constellations shown in Fig. 15(b) and (c), the results demonstrate that only the authorized users can successfully decrypt the received signal, while the illegal receiver with the wrong keys cannot get the useful information and BERs are always staying at approximately 0.5. For the 3-D 16QAM rectangular constellation mapping, the inner pattern of the illegal receiver's constellation diagram looks denser than the external pattern due to the visual effect caused by the gap between the outer distributed region and the inner distributed region.

Overall, the proposed three-step encryption scheme can be universally applicable to encrypt any CO-OFDM system that employs the 3-D constellation, and it also provides promising insights that the proposed encryption scheme along with the 3-D constellation can simultaneously enhance the security and improve the transmission performance of the CO-OFDM system.

V. Conclusion

In this paper, a novel secure strategy for CO-OFDM system at the physical layer has been proposed and experimentally demonstrated, where a 5-D hybrid hyperchaotic system and 3-D constellation design techniques are employed to improve the system security and transmission performance simultaneously. The three-step encryption is controlled by the chaotic sequences generated from two 1-D logistic maps and one 3-D Hénon map. The proposed encryption scheme can provide a huge key space

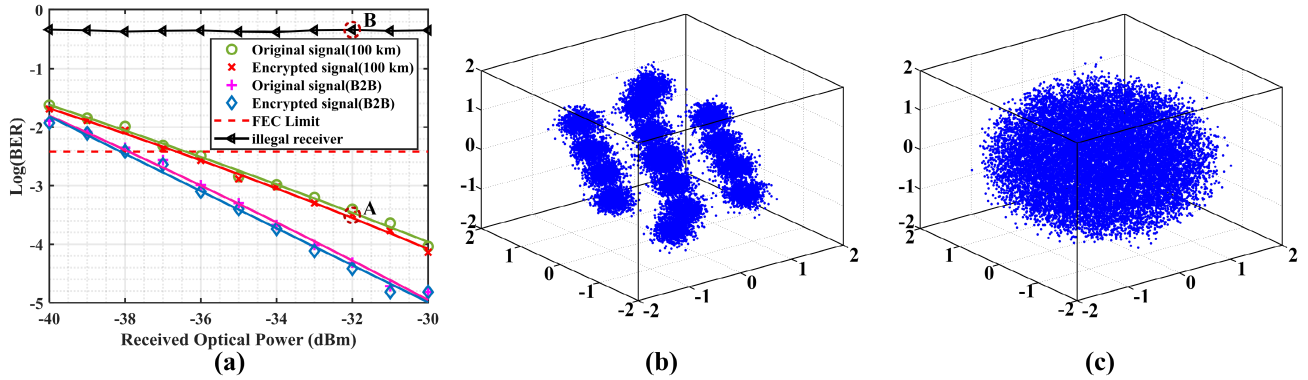

Fig. 14. (a) BER curves for different OFDM signals versus the received optical power; (b) the received constellation corresponding to point A in (a); (c) the received constellation corresponding to point B in (a).

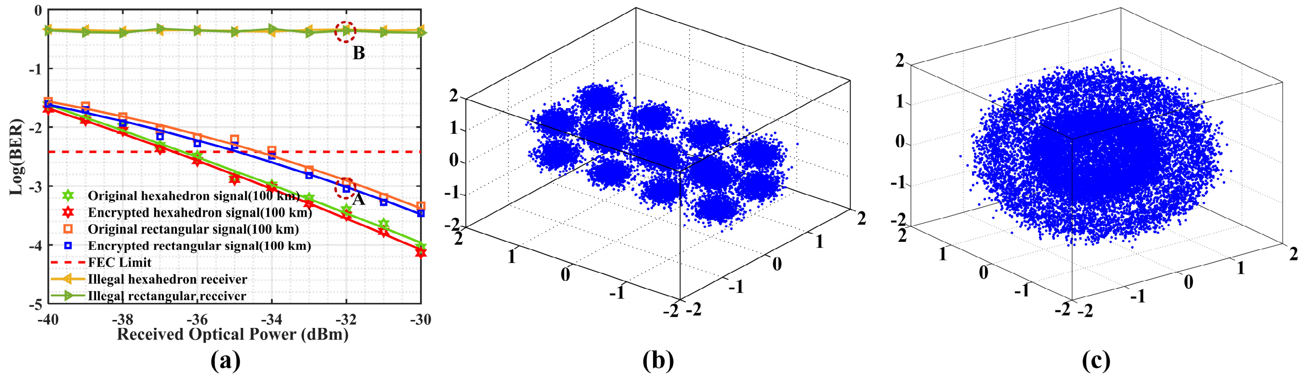

Fig. 15. (a) BER curves for OFDM signals with 3-D hexahedron constellation and 3-D rectangular constellation versus the received optical power; (b) the received constellation corresponding to point A in (a); (c) the received constellation corresponding to point B in (a).

of ~10^{133} which removes the possibility of any successful brute-force attacks. Meanwhile, a novel 3-D regular hexahedron signal constellation has been designed to improve the transmission performance of the CO-OFDM system. In order to verify the feasibility of our encryption schemes, 144 Gb/s 16QAM CO-OFDM signals have been successfully experimentally demonstrated over a 100 km SSMF transmission. The experimental results further prove the high sensitivity and effective encryption of the proposed encryption scheme. The designed 3-D regular hexahedron 16QAM constellation can significantly improve the overall performance of the OFDM system, which shows its great potential for the physical layer security enhancement and transmission performance improvement in future CO-OFDM systems.

References

[1] J. Armstrong, "OFDM for optical communications," *J. Lightw. Technol.*, vol. 27, no. 3, pp. 189-204, Feb. 2009.

[2] N. Cvijetic, "OFDM for next-generation optical access networks," *J. Lightw. Technol.*, vol. 30, no. 4, pp. 384-398, Feb. 2012.

[3] W. Shieh, "OFDM for flexible high-speed optical networks," *J. Lightw. Technol.*, vol. 29, no. 10, pp. 131-138, Jan. 2007.

[4] Z. X. Wang, J. Chang, and P. R. Prucnal, "Theoretical analysis and experimental investigation on the confidentiality of 2-D incoherent optical CDMA system," *J. Lightw. Technol.*, vol. 28, no. 12, pp. 1761–1769, Apr. 2010.

[5] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inform. Forensic Secur.*, vol. 6, no. 3, pp. 725–736, Apr. 2011.

[6] S. Bravyi, D. Gosset, and R. Kongig, "Quantum advantage with shallow circuits," *Science*, vol. 362, no. 6412, pp. 308-311, Oct. 2018.

[7] A. K. Zhao, N. Jiang, S. Q. Liu, Y. Q. 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.

[8] N. Jiang, A. K. Zhao, C. P. Xue, J. M. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, pp. 1536-1539, Apr. 2019.

[9] L. S. Wang, X. X. Mao, A. B. Wang, Y. C. Wang, Z. S. Gao, S. S. Li, and L. S. Yan, "Scheme of coherent optical chaos communication," *Opt. Lett.*, vol. 45, pp. 4762-4765, 2020.

[10] M. Cheng, L. Deng, X. Gao, H. Li, M. Tang, S. Fu, P. Shum, and D. Liu, "Security-enhanced OFDM-PON using hybrid chaotic system," *IEEE Photon. Technol. Lett.*, vol. 27, no. 3, pp. 326-329, Feb. 2015.

[11] L. Zhang, B. Liu, X. Xin, Q. Zhang, J. Yu, and Y. Wang, "Theory and performance analyses in secure CO-OFDM transmission system based on two-dimensional permutation," *J. Lightw. Technol.*, vol. 31, no. 1, pp. 74-80, Jan. 2013.

[12] A. Hajomer, X. Yang, and W. Hu, "Secure OFDM transmission precoded by chaotic discrete hartley transform," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7901209.

[13] Z. Shen, X. Yang, H. He, and W. Hu, "Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos," *IEEE Photon. J.*, vol. 8, no. 3, Jun. 2016, Art. no. 7904609.

[14] J. Zhong, X. Yang, and W. Hu, "Performance-improved secure OFDM transmission using chaotic active constellation extension," *IEEE Photon. Technol. Lett.*, vol. 29, no. 12, pp. 991–994, Jun. 2017.

[15] 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, Aug. 2018.

[16] T. Wu, C. Zhang, C. Chen, H. Hou, H. Wei, S. Hu, and K. Qiu, "Security enhancement for OFDM-PON using Brownian motion and chaos in cell," *Opt. Express*, vol. 26, no. 18, pp. 22857–22865, Sep. 2018.

[17] W. Zhang, C. Zhang, C. Chen, and K. Qiu, "Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1524– 1530, May 2017.

[18] C. Zhang, W. Zhang, C. Chen, X. He, and K. Qiu, "Physical-Enhanced Secure Strategy for OFDMA-PON Using Chaos and Deoxyribonucleic Acid Encoding," *J. Lightwave Technol.*, vol. 36, no. 9, pp. 1706–1712, May. 2018.

[19] L. Zhang, B. Liu, and X. Xin, "Secure optical generalized filter bank multi-carrier system based on cubic constellation masked method," *Opt. Lett.*, vol. 40, no. 12, pp. 2711-2714, Jun. 2015.

[20] L. Zhang, B. Liu, and X. Xin, "Secure coherent optical multi-carrier system with four-dimensional modulation space and Stokes vector scrambling," *Opt. Lett.*, vol. 40, no. 12, pp. 2858-2861, Jun. 2015.

[21] L. Zhang, X. Xin, B. Liu, and J. Yu, "Physical-enhanced secure strategy in an OFDM-PON," *Opt. Express*, vol. 20, no. 3, pp. 2255-2265, Jan. 2012.

[22] X. Song, B. Liu, H. Zhang, R. Ullah, Y. Mao, J. Ren, S. Chen, J. Zhang, J. Zhao, S. Han, X. Liu, D. Zhao, and X. Xin, "Security-enhanced OFDM-PON with two-level coordinated encryption strategy at the bit-level and symbol-level," *Opt. Express*, vol. 28, no. 23, pp. 35061-35073, Nov. 2020.

[23] J. Zhao, B. Liu, Y. Mao, R. Ullah, J. Ren, S. Chen, L. Jiang, S. Han, J. Zhang, and J. Shen, "High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization," *Opt. Express*, vol. 28, no. 14, pp. 21236-21246, Jul. 2020.

[24] S. Li, M. Cheng, L. Deng, S. Fu, M. Zhang, M. Tang, P. Shum, and D. Liu, "Secure strategy for OFDM-PON using digital chaos algorithm with fixed-point implementation," *J. Lightw. Technol.*, vol. 36, no. 20, pp. 4826–4833, Oct. 2018.

[25] L. Deng, M. Cheng, X. Wang, H. Li, M. Tang, S. Fu, P. Shum, and D. Liu, "Secure OFDM-PON system based on chaos and fractional Fourier transform techniques," *J. Lightw. Technol.*, vol. 32, no. 15, pp. 2629-2635, Aug. 2014.

[26] J. Ren, B. Liu, D. Zhao, S. Han, S. Chen, Y. Mao, Y. Wu, X. Song, J. Zhao, X. Liu, and X. Xin, "Chaotic constant composition distribution matching for physical layer security in a PS-OFDM-PON," *Opt. Express*, vol. 28, no. 23, pp. 39266-39276, Dec. 2020.

[27] S. G. Kang, "An OFDM with 3-D signal mapper and 2-D IDFT modulator," *IEEE Commun. Lett.*, vol. 12, no. 12, pp. 871-873, Dec. 2008.

[28] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[29] Alia Karim Abdul Hassan, "Proposed hyperchaotic system for image encryption," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 37-40, 2016.

[30] Z. Chen, J. Liu, S. Li, and S. G. Kang, "New 3D 16-ary signal constellations and their symbol error probabilities in AWGN and Rayleigh fading channels," *Wireless Commun. Mobile Comput.*, vol. 2018, Aug. 2018, Art. No. 7178631.

[31] X. Li, W. Li, J. Lei, L. Cheng, "A novel physical layer encryption algorithm based on three dimensional constellation rotation in OFDM system," *Acta Electronica Sinica*, vol. 45, no. 12, pp. 2873-2880, 2017.

[32] G. D. Forney, L. Wei, "Multidimensional constellations. I. Introduction, figures of merit, and generalized cross constellations," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 6, pp. 877-892, Aug. 1989.

[33] H. Wu, J. Zhang, and H. Song, "A lattice based approach to the construction of multi-dimensional signal constellations," *Acta Electronica Sinica*, vol. 42, no. 9, pp. 1672-1679, 2014.

[34] J. G. Proakis, M. Salehi, *Digital Communications*, New York, NY, USA: McGraw Hill, 2008, pp. 160-289.

[35] S. G. Kang, Z. X. Chen, J. Y. Kim, J. S. Bae, and J. S. Lim, "Construction of Higher-Level 3-D Signal Constellations and Their Accurate Symbol Error Probabilities in AWGN," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 6267-6272, Aug. 2011.

[36] Lei Deng, Xiaolong Wang, Cong Zhou, Ming Tang, Songnian Fu, Minming Zhang, Perry Ping Shum, and Deming Liu, "Experimental Demonstration of a 16.27 Gb/s 2-D Coherent Optical OFDM System With 3-D Signal Mapper and 2-D IFFT Modulator," *J. Lightw. Technol.*, vol. 34, no.4, pp. 1177-1183, Feb. 2016.

[37] R. P. Giddings, X. Q. Jin, E. Hugues-Salas, E. Giacoumidis, J. L. Wei, and J. M. Tang, "Experimental demonstration of a record high 11.25Gb/s real-time optical OFDM transceiver supporting 25km SMF end-to-end transmission in simple IMDD systems," *Opt. Express*, vol. 18, no. 6, pp. 5541-5555, Mar. 2010.