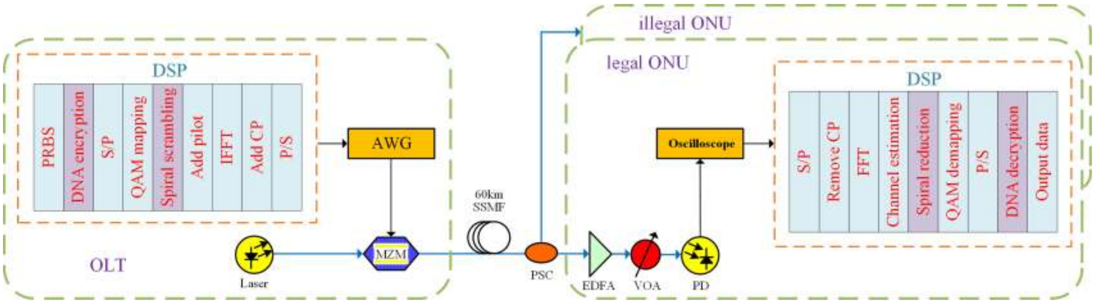
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

A Novel Hybrid Secure Method Based on DNA Encoding Encryption and Spiral Scrambling in Chaotic OFDM-PON

Volume 12, Number 3, June 2020

Yaoqiang Xiao
Yating Chen
Caixia Long
Jin Shi
Jie Ma
Jing He



DOI: 10.1109/JPHOT.2020.2987317

A Novel Hybrid Secure Method Based on DNA Encoding Encryption and Spiral Scrambling in Chaotic OFDM-PON

**Yaoqiang Xiao, Yating Chen, Caixia Long, Jin Shi, Jie Ma,
and Jing He**

College of Computer Science and Electronic Engineering, Hunan University, Changsha
410082, China

DOI:10.1109/JPHOT.2020.2987317

Manuscript received February 23, 2020; revised April 7, 2020; accepted April 8, 2020. Date of publication April 17, 2020; date of current version April 28, 2020. This work was supported in part by the National Natural Science Foundation of China under Grants 61975054 and 61775054, in part by the Hunan Provincial Natural Science Foundation of China under Grant 2017JJ2047. Corresponding author: Yaoqiang Xiao (e-mail: yaoqiangxiao@hnu.edu.cn).

Abstract: This paper proposes a novel hybrid secure method based on improved deoxyribonucleic acid (DNA) encoding encryption and spiral scrambling in chaotic OFDM-PON for enhancing the physical-layer security. In the improved DNA encoding encryption, the odd-even cross-bit DNA encoding, base scrambling and base-level substitution are determined by chaotic sequences. For each binary and base, the selected encoding rules and base scrambling methods are dynamically changing, which enhances the robustness against malicious attacks by attackers. In the spiral scrambling process, the QAM symbol matrix is divided into several blocks, and these blocks are scrambled. In the scrambling of the plural matrix, the position where the spiral starts and the orientation and direction of the traversal are also controlled by the chaotic sequences. By employing DNA encoding encryption and spiral scrambling, a key space of $\sim 10^{135}$ can be achieved in the multi-fold encryption of the proposed scheme, which can improve the physical-layer security. The encrypted 16-QAM OFDM data are successfully transmitted over a 60-km SSMF in OFDM-PON. The simulation results demonstrate that it has better BER performance at the BER of 10^{-3} than other schemes. The proposed encryption method can effectively protect data from attacks by eavesdroppers or illegal users.

Index Terms: Spiral scrambling, deoxyribonucleic acid (DNA) encoding encryption, chaos, OFDM-PON, secure communication.

1. Introduction

Passive optical network (PON) is an advanced defense solution to figure out the high bandwidth requirements of next-generation multiuser access networks, and orthogonal frequency division multiplexing (OFDM) has strong anti-multipath interference capability and is widely used in wired and wireless systems. Thus, under the impetus of the increasing demand for data transmission in modern optical communication systems, the orthogonal frequency division multiplexing passive optical network (OFDM-PON) has become a preeminent candidate for meeting the demands of next-generation networks due to its high spectrum utilization, dispersion tolerance, low bandwidth requirements, anti-multipath interference, and high signal transmission capability [1]–[3]. At the same time, the growing demand for information sharing has made communication security a focus of concern. Typically, the traditional encryption techniques of OFDM-PON are directly targeted at the upper layer, and the transmitted signal in the physical layer is transparent to eavesdroppers. Therefore, the system is vulnerable to attackers. For improving the security of digital signal processing (DSP)-based OFDM-PON, physical-layer encryption has attracted substantial research interests [4].

In recent years, many secure schemes have been proposed [5], [6]. By virtue of its high pseudo randomness, unpredictability, and sensitivity to initial values [7], chaos is applied to the security encryption schemes in the electrical and optical domains [8]–[10]. In the optical domain, the encryption techniques include chaotic laser communication [11] and exclusive OR (XOR) disturbance [12]. In the electrical domain, the related encryption techniques that are used in wireless communication systems are based on chaos and hyper-chaos, but the randomness of a chaotic sequence can be affected by the limited precision of the computer because the data are directly encrypted with chaos. To improve the encryption performance, electronic domain encryption schemes based on chaos have been studied, such as constellation encryption, precoding, symbol and subcarrier scrambling, and so on. Various approaches are available for constellation encryption, such as chaotic shifting of the quadrature amplitude modulation (QAM) constellation [13], and chaotic active constellation extension [14]. Recently, pilot-aided key agreement, along with chaotic constellation transformation technique, is demonstrated to enhance the security of physical layer [15]. For precoding, many encryption schemes have been proposed, such as chaotic discrete Hartley transform [16], discrete Fourier transform [17] and chaotic Walsh-Hadamard transform [18]. In addition to improving the physical-layer security, precoding is an effective method for reducing the peak-to-average power ratio [19], [20]. Involving symbol and subcarrier scrambling, many encryption schemes are studied, such as Brownian motion for scrambling the QAM symbols [21], partial transmission sequence technique [22], block dividing with chaos and dynamic key [23], chaotic pseudo-random RF subcarriers [24], and hybrid chaotic confusion and diffusion [25]. There are many other encryption schemes in combination with chaos, e.g., fixed-point digital chaos algorithm [26], time-frequency domain encryption with selected mapping scheme [27], piecewise chaotic permutation method [28], and polar-coded chaotic encryption method [29]. However, the basic form of the data, i.e., bit, is not taken into consideration in these encryption methods, and the security of the data will be reduced. A type of bit-level encryption, i.e., deoxyribonucleic acid (DNA) encoding encryption [30], can improve physical-layer security. Since DNA has the characteristics of a satisfactory amount of storage, massive parallel processing capabilities, and ultra-low power consumption, the combination of chaos and DNA encoding encryption is proposed in OFDM-PON system [31]. However, only a few combination researches have been conducted on combining DNA encoding encryption and chaos in OFDM-PON.

In this paper, a hybrid secure method based on improved DNA encoding encryption and spiral scrambling scheme in chaotic OFDM-PON system is proposed, which can enhance the physical-layer security. Each pseudo-random binary sequence (PRBS) will undergo DNA encoding encryption initially. The binary sequences are converted to bases according to DNA encoding rules, where the odd-even cross-bit DNA encoding is applied. Then, the bases are subjected to base scrambling and after base-level substitution, the scrambled bases are restored to binary sequences via base-binary transformation, namely, the data are bit-level encrypted. In the spiral scrambling process, the scrambled binary data are mapped into a QAM symbol matrix. Then, an element is randomly selected from the QAM symbol matrix, and spiral traversal is conducted around the selected element according to a specified orientation and direction. After the spiral traversal, the traversed elements are rearranged into a matrix. The choice of DNA encoding rules and base scrambling methods, the selection of starting element, and the determination of orientation and direction in spiral scrambling are all controlled by the chaotic system. The simulation results demonstrate that physical-layer-secure OFDM data can be transmitted over a 60-km standard single mode fiber (SSMF), and the proposed scheme can defend against illegal users and provide an effective security enhancement of OFDM-PON.

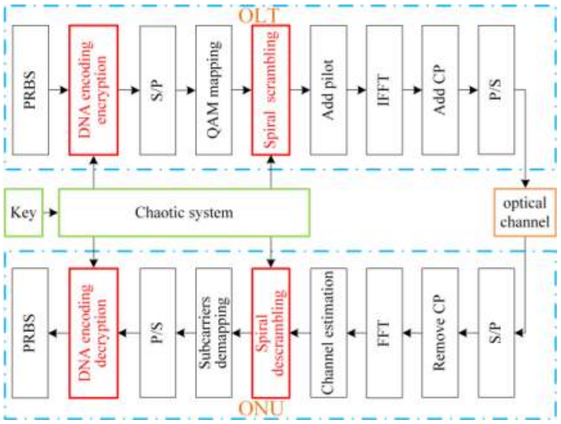


Fig. 1. Schematic diagram of the proposed method based on DNA encoding encryption and spiral scrambling.

TABLE 1
DNA Encoding and Decoding Rules

Rule	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
00	A	A	C	G	C	G	T	T
01	C	G	A	A	T	T	C	G
10	G	C	T	T	A	A	G	C
11	T	T	G	C	G	C	A	A

2. Principle

The schematic diagram of the hybrid secure method based on DNA encoding encryption and spiral scrambling is illustrated in Fig. 1. In OFDM-PON, the optical line terminal (OLT) and the optical network unit (ONU) are the basic units, which act as a transmitter and a receiver, respectively. At the OLT, PRBS is applied as the original input data. First, the binary sequence will be transformed according to the DNA encoding rules and will be encrypted based on chaos and base scrambling methods. After serial-to-parallel conversion (S/P) and QAM modulation, a QAM symbol matrix can be obtained. Second, spiral scrambling is performed on elements of the QAM matrix, which can yield a new QAM matrix. After the pilots have been added, inverse fast Fourier transform (IFFT) modulation is applied to the signal. Then, by adding the cyclic prefix (CP) and performing parallel-to-serial (P/S) conversion, the signal can be transmitted.

2.1 DNA Encoding Encryption Process

A DNA sequence consists of four types of nucleic acid bases: adenine (A), guanine (G), cytosine (C) and thymine (T). These DNA bases follow the Watson-Crick principle. According to the principle, “A” and “T” are two complementary base pairs, as are “C” and “G”. Typically, two bits are used to encode each of the DNA bases, namely, “00”, “01”, “10”, and “11” are used to encode bases “A”, “G”, “C”, and “T”, respectively. Thus, there are twenty-four encoding rules. However, since for binary encoding, “0” and “1” are complementary pairs, “00” and “11”, are complementary pairs, as are “01” and “10”. Therefore, to accommodate this complementary relationship, the rules that do not satisfy this complementarity relationship should be removed from the set of twenty-four encoding rules. The remaining eight rules satisfy the requirements, which are listed in Table 1.

The improved DNA encoding encryption process is shown in Fig. 2. The process consists of five main parts: binary-base transformation, key base sequence generation, base scrambling, base-level substitution and base-binary transformation, in which S_1, S_2, S_3, XL and K are generated by the chaotic system. PRBS is transformed to bases by odd-even cross-bit DNA encoding according to

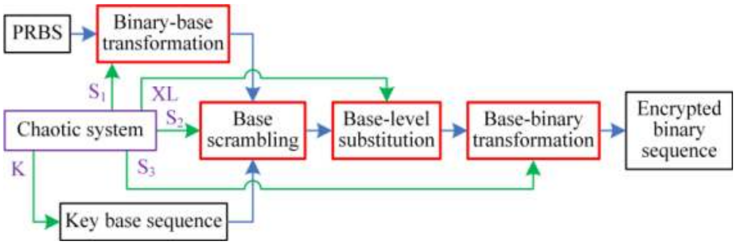


Fig. 2. Improved DNA encoding encryption process.

the encoding rules, where the selection of DNA encoding rules is controlled by parameter sequence S_1. At the same time, the sequence K is used as the key base sequence. For base scrambling, the parameter sequence S_2 controls the combination of the transformed DNA sequence and the key base sequence K, and a new DNA sequence can be obtained. After the base-level substitution applied on the new DNA sequence according to the sequence XL, the parameter sequence S_3 controls the rules of base-binary transformation, and the new DNA sequence is converted into binary data again.

In the DNA encoding encryption process, if there are many identical consecutive binary pairs in a pseudo-random binary sequence, many identical bases will be produced after binary-base transformation, namely, if there are many "11" pairs in the sequence, many "T" bases will be generated by the pseudo-random DNA encoding rules according to rule 1 and the number of "T" bases is the largest in the DNA sequence. If a fixed encoding rule is used in binary-base transformation, it will weaken the security and the transmitted information will be easier for an eavesdropper to intercept. In summary, the dynamic DNA encoding method should be considered. For every binary bit pair, the encoding rules are changed and this change is based on the control parameters S_1 and S_3 being chaotic sequences. Each value of a sequence corresponds to the reselection of one encoding rule from Table 1. Accordingly, the base scrambling of DNA sequence and key base sequence K is also pseudo-random, which is based on the control parameter sequence S_2. Even if the eavesdropper cracks one or several of the encoding rules, the overall trend is unpredictable; hence, the possibility of being cracked will be substantially reduced. The confidentiality is further improved, and the key space is enlarged.

To obtain the control parameters S_1, S_2, S_3, the key base sequence K and the sequence XL in the proposed method, a spatially generalized Logistic system is used, which is defined as follows [32],

$$x(m+1,n)+\omega\cdot x(m,n+1)=1-\mu\cdot((1+\omega)\cdot x(m,n))^2 \tag{1}$$

where m is the discrete time index, μ is a positive parameter, ω is a real constant, n is the lattice site index and $n=1,2,\ldots,N$, where N is the chaotic system size, which is typically determined by the number of states. In the proposed scheme, since this chaotic system will be used later, N is set to 7. In order to reduce the impact of periodic windows on the system, a series of nonlinear operations are conducted on the random sequence.

2.1.1 Binary-Base Transformation: In normal DNA encoding, every two consecutive binaries in the sequence are a group, and each group of binaries is encoded to bases in turn by random DNA encoding rules. Different from the normal DNA encoding, the odd-even cross-bit DNA encoding is applied in the proposed scheme to increase the complexity of algorithm for security. The binary sequence is divided into two subsequences according to their odd and even positions in the sequence, and the normal DNA encoding is conducted on two subsequences respectively. Then, the encoded base sequences are spliced and combined in sequence.

How each binary bit pair is mapped to a base depends on the selection of the encoding rules by the control parameter sequence S_1, where the elements of the parameter sequence S_1 are in an integer set $\{1,\ldots,8\}$. The chaotic integer sequence S_1 is generated by using the state $x(m,1)$ of

TABLE 2
Addition (+) Operation

Addition (+)	**A**	**C**	**T**	**G**
A	C	A	G	T
T	G	T	C	A
C	A	C	T	G
G	T	G	A	C

TABLE 3
Subtraction (-) Operation

Subtraction (-)	**A**	**C**	**T**	**G**
A	C	G	A	T
T	G	T	C	A
C	A	C	T	G
G	T	A	G	C

TABLE 4
Exclusive OR (XOR) Operation

Exclusive OR (XOR)	**A**	**C**	**T**	**G**
A	A	C	T	G
T	T	G	A	C
C	C	A	G	T
G	G	T	C	A

the spatially generalized Logistic system. And S_1 can be calculated via the following formula,

$$S_1 = \mathrm{mod}(ceil(x(m, 1) \cdot 10^{15}), 8) + 1 \tag{2}$$

where $ceil(\cdot)$ rounds the element to the nearest integer toward infinity and $\mathrm{mod}(R, 8)$ returns the remainder of R divided by 8.

2.1.2 Key Base Sequence Generation: In the base scrambling, a key base sequence is necessary. Facilitated by the spatially generalized Logistic system, the key base sequence $K = \{k\}$ is generated by utilizing the chaotic state $x(m, 2)$, and the generation process can be expressed as follows,

$$\tau = \mathrm{mod}(Extract(x(m, 2), i\_th), 4) + 1 \tag{3}$$

$$k ='' T''/''G''/''C''/''A'', \quad \text{when} \quad \tau = 1/2/3/4 \tag{4}$$

2.1.3 Base Scrambling: There are three base scrambling operations of the DNA sequence and the key base sequence K that are controlled by the parameter sequence S_2, namely, "addition (+)", "subtraction (-)", and "Exclusive OR (XOR) ", which are specified in Tables 2, 3, and 4. The parameter sequence S_2 determines which operation is chosen in the base scrambling. As the value of the parameter sequence S_2 changes, the base scrambling operation that is performed each time also changes. Each element of S_2 is in the set $\{1, 2, 3\}$ and corresponds to a base scrambling operation. The state $x(m, 3)$ of the chaotic system is used to generate the chaotic integer sequence S_2, which has the following formula,

$$S_2 = \mathrm{mod}(Extract(x(m, 3), i\_th), 3) + 1 \tag{5}$$

where the function $Extract(x, i\_th)$ returns the i_th digit of the fractional part of x, which is an integer.

2.1.4 Base-Level Substitution: Although the selection of the base scrambling method is pseudo-random, some identical bases will be produced continuously. To reduce the production of identical bases in succession, the base-level substitution process is applied after the base scrambling, which is also controlled by the Logistic system. In this process, the iteration state $x(m, 4)$ of the chaotic system is performed to obtain the desired chaotic sequence XL. The elements xl of the sequence XL produced directly by the spatially generalized Logistic system are all decimal numbers and are in the range of $(-1, 1)$. The values of chaotic sequence XL should be mapped to the discrete domain $\{0, 1\}$ from the continuous domain $(-1, 1)$. The process is defined as follows,

$$xl(i) = \begin{cases} 1, \text{ if } x(i, 4) > 0 \\ 0, \text{ if } x(i, 4) \leq 0 \end{cases} \tag{6}$$

Due to the properties of the DNA bases, the values of the sequence XL are used to complement the processed base sequence. If the i_th element of XL is 0, the i_th base of the base sequence is unchanged. In contrast, if the i_th element of XL is 1, the i_th base of the base sequence becomes its complementary base, namely, "A" and "T" are interchanged, and "C" and "G" are interchanged.

2.1.5 Base-binary Transformation: When the DNA bases are converted to the binary sequence, the control parameter sequence S_3 is used to select the rules of base-binary transformation and the element of S_3 also returns an integer from $\{1, \ldots, 8\}$. The corresponding mapping relationship is presented in Table 1. S_3 is generated by using the state $x(m, 5)$, which is described as follows,

$$S_3 = \text{mod}(ceil(x(m, 5) \cdot 10^{15}), 8) + 1 \tag{7}$$

In DNA encoding encryption, the initial values of the spatially generalized Logistic system and the system parameters μ and ω are used as security keys.

At the ONU, the decryption process is the reverse process of the DNA encoding encryption. The encoding rules for binary-base transformation of pseudo-random encrypted signals are controlled by S_3 (from Table 1). The transmitter and the receiver share security keys. If the initial values and the system parameters μ and ω are known, the same key base sequence K used in DNA encoding encryption will be recovered by the chaotic system. The input encoded DNA sequence undergoes the base-level substitution according to the sequence XL and is combined with the key base sequence K via base scrambling to yield a new DNA sequence. The base scrambling methods here are the inverse of the base scrambling methods that are used in DNA encoding encryption (from Table 2, 3, and 4), and S_2 controls which base scrambling method is selected. And then, the obtained DNA sequence is restored to a binary sequence according to the DNA decoding rules, which are controlled by S_1 (from Table 1).

Then, the binary sequence undergoes serial-to-parallel (S/P) conversion and is mapped into a QAM symbol matrix.

2.2 Spiral Scrambling Encryption Process

The obtained QAM matrix contains multiple elements, and each complex number in the QAM symbol matrix is converted into a decimal integer number. Since the modulation format of the system is 16-QAM, the range of decimal numbers to which symbols are converted is $(0, 15)$. The mapping rule for mapping symbols to decimal numbers is self-defining. Then, a matrix P with all elements in decimal-number form is obtained. The spiral scrambling encryption process is illustrated in Fig. 3.

2.2.1 Block Scrambling: The size of the matrix P is $M \times N$, which is the same as the size of the QAM symbol matrix. The block scrambling process of the matrix is as follows:

① Dividing the matrix P into blocks of size $m \times n$. The total number of obtained blocks is $l = \frac{M \times N}{m \times n}$. The i_th block is written as $G_i^{m \times n}$, where $i = 1, 2, \ldots, l$.

② Scrambling the obtained blocks. The indices of the blocks are queued into a sequence, and the values in the sequence are scrambled to generate a new sequence $f^{1 \times l} = \{f(i)\}$, where

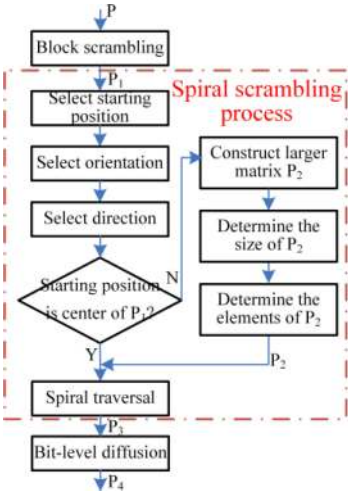


Fig. 3. Spiral scrambling encryption process.

$f(i) \in \{1, 2, \ldots, l\}$, $i = 1, 2, \ldots, l$. The sequence $f^{1\times l} = \{f(i)\}$ is used as the index sequence of the new block arrangement matrix to scramble the original small blocks $G_i^{m\times n}$. The scrambled blocks satisfy $W_i^{m\times n} = G_{f(i)}^{m\times n}$. All l new blocks $W^{m\times n}$ are recombined into a new matrix P_1, which is also of size $M \times N$.

2.2.2 Spiral Scrambling Process: Based on the processing of the above data, an $M \times N$ matrix P_1 is obtained. Then, the spiral scrambling process is applied to the matrix P_1 as follows:

① Selecting the starting position. First, the position of an element of the matrix should be determined, which depends on the chaotic system. The state $x(m, 6)$ of the spatially generalized Logistic system is utilized to generate the chaotic integer sequence S_4. Only some of these numbers will be used as control parameters to conduct the spiral scrambling. And the calculation process of S_4 can be expressed as

$$S_4 = \mathrm{mod}(floor(abs(x(m, 6)) \cdot 10^{15}), 16) + 1 \tag{8}$$

where $floor(\cdot)$ rounds each element to the nearest integer that is less than or equal to the element. $S_4 = \{s_4\}$ is a random number set, and $s_4 \in \{1, 2, \ldots, 16\}$. The i_th, j_th, k_th, and l_th elements of the chaotic sequence S_4 are selected as control parameters, which are denoted as a_1, a_2, a_3, and a_4, respectively. To better control the spiral scrambling process, these numbers must be further manipulated. a_1 and a_2 are used to control the row and column of p_1, which is the selected element in the matrix P_1. The position of p_1 is (D_x, D_y), where $D_x = a_1$ and $D_y = a_2$.

② Selecting the orientation. Traversal can begin at the top, bottom, left or right of an element; hence, the control parameter a_3 can be utilized to control the orientation from which the traversal begins. However, there are only four orientations and $a_3 \in \{1, 2, \ldots, 16\}$. The following process should be performed to obtain D_z, which is in the set $\{1, 2, 3, 4\}$,

$$D_z = \mathrm{mod}(a_3, 4) + 1 \tag{9}$$

The correspondence between D_z and the orientations is as follows, "1" → "top", "2" → "bottom", "3" → "left", and "4" → "right".

③ Selecting the direction. After determining the starting orientation of the traversal, the direction of the traversal should be selected. The clockwise and counterclockwise directions can be used to traverse all elements of the matrix. To control the direction, a similar operation to the operation that was performed on a_3 is performed on a_4, and the control parameter D_u can be obtained as follows,

$$D_u = \mathrm{mod}(a_4, 2) + 1 \tag{10}$$

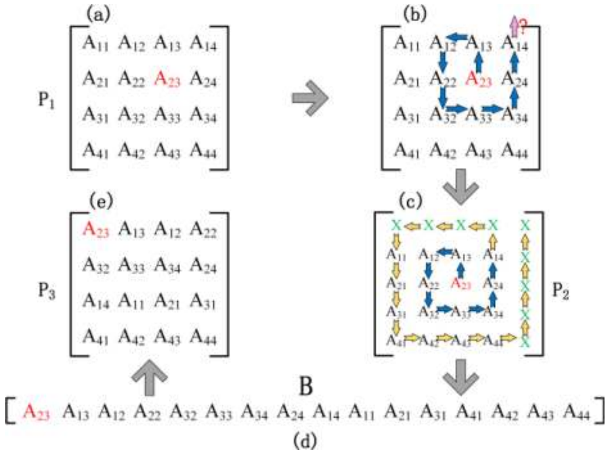


Fig. 4. Example of spiral scrambling (“X” represents the special number).

After the selected element and the traversal direction have been obtained, the first few layers of element traversal can proceed normally. However, the position of the selected element p_1 is not always at the center of the matrix. Once the traversal has reached the matrix boundary, the next position to be traversed is outside the matrix, which will affect the whole process. To solve the problem, matrix P_1 is expanded into a larger square matrix P_2, whose size is determined as follows:

- Determining the size of matrix P_2. In matrix P_1, the distances of the selected element from the boundaries can be measured, which are denoted as a, b, c, and d. The largest distance is expressed as

$$MAX = \max\{a, b, c, d\} \tag{11}$$

The size of matrix P_2 is

$$SL = 2 \times MAX + 1 \tag{12}$$

- Determining the elements of matrix P_2. Based on the matrix P_1, the selected element p_1 is set as the matrix center, and the matrix is expanded according to the calculated size to obtain the expanded matrix P_2. The special numbers are utilized to fill the matrix in the expansion to distinguish from the original elements.

In the newly constructed matrix P_2, spiral traversal is performed on all elements, and the elements that are read via spiral traversal are stored in an array, which is denoted as B. The elements of array B that belong to matrix P_1 are extracted in order and these extracted elements are rearranged in the form of an $M \times N$ matrix to obtain the new shuffled matrix P_3.

Regarding the storage space, matrix P_2 is not independently constructed from matrix P_1, and matrix P_2 is expanded based on P_1. Therefore, matrices P_1 and P_2 will point to a common storage space. In addition to the space that is occupied by matrix P_1, matrix P_2 makes additional extensions and takes up slightly more space. Compared to constructing a new matrix, expansion of the original matrix P_1 will save much space, and it will not cause excessive space occupation.

Fig. 4 presents an example of the spiral scrambling. The size of matrix P_1 is set to 4×4. A_{23} is selected randomly as the starting element of the spiral traversal, which is marked in red in Fig. 4(a). Assuming that the selected orientation is “top” and the traversal direction is counterclockwise, the path of the element traversal is illustrated in Fig. 4(b), in which the blue arrows indicate the traversal trajectory of the first-layer elements. When traversing to the boundary element A_{14}, no elements can be traversed in the normal direction, as indicated by the pink arrow. Therefore, it is impossible to proceed according to the normal path. As explained above, centering on the element A_{23}, the distances to the boundaries should be calculated and compared. It is found that the largest distance is 2, i.e., $MAX = 2$. Hence, the size of matrix P_2 is $2 \times MAX + 1 = 5$. And then, on the basis of the

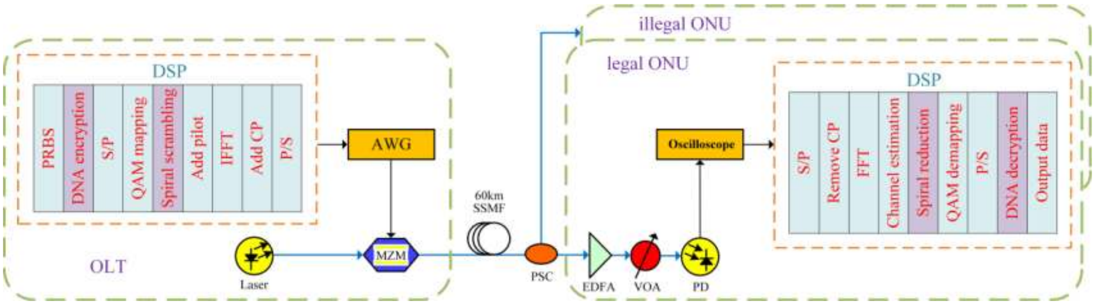


Fig. 5. Simulation setup of the proposed chaotic OFDM-PON based on DNA encryption and spiral scrambling.

matrix P_1, A_{23} is taken as the center element for expansion according to the calculated size 5 to obtain the expanded matrix P_2, filling with the special number "X" in the expansion. Via this approach, if the spiral traversal is conducted with A_{23} as the starting point, all the elements in the matrix can be traversed layer by layer as originally planned, as shown in Fig. 4(c). The blue arrows represent the traversal of the first layer of elements, and the yellow arrows represent the traversal of the second layer of elements. Then, the traversed elements are arranged in an array B in Fig. 4(d), and the special number elements are removed, thereby leaving only useful data. Finally, the elements in array B are reshaped into a matrix P_3, as illustrated in Fig. 4(e).

2.2.3 Bit-level Diffusion: In addition, to further improve the security of the system, matrix P_3 finally undergoes bit-level diffusion, which can enlarge the key space and improve the ability to resist malicious attacks. In order to obtain a sequence that can complete bit-level diffusion, the state $x(m, 7)$ of the spatially generalized Logistic system is employed, and the sequence values of $x(m, 7)$ after the system iteration for $M \times N$ times constitute the desired chaotic matrix YS. The size of matrix YS is $M \times N$, and the elements of matrix YS are also all decimal numbers that are in the range of $(-1, 1)$. The elements of chaotic matrix YS are mapped to the discrete domain $\{0, 1, \ldots, 15\}$ from the continuous domain $(-1, 1)$ according to the following formula,

$$U = \mathrm{mod}(ceil(YS \times 10^4), 16) \tag{13}$$

Therefore, U is also an $M \times N$ matrix, whose elements are integers within the set $\{0, 1, \ldots, 15\}$. The XOR operation is performed on matrix P_3 and matrix U to obtain a scrambled $M \times N$ matrix P_4, which is expressed as follows,

$$P_4 = P_3 \oplus U \tag{14}$$

3. Simulation Setup

Fig. 5 illustrates the simulation setup of the proposed chaotic OFDM-PON, which is based on DNA encryption and spiral scrambling. In order to test and verify the feasibility of the proposed encryption scheme, a legitimate user and an illegal user are employed, and a series of simulation software are used to simulate the proposed chaotic OFDM-PON. The simulation tools are MATLAB and OptiSystem software. At OLT, the length of the binary data is 1024 and hundreds of frames of data are used for transmission. For each frame, the IFFT/FFT size is 1024. Among the 1024 subcarriers, 16 subcarriers are used to carry the pilots for channel estimation and 512 subcarriers are allocated for the 16-QAM data, of which 256 subcarriers carry raw 16-QAM data and the remaining 256 subcarriers are applied as the corresponding complex conjugates for Hermitian symmetry. The pilots are inserted into the symbol data to be transmitted, which are selected from the pilot set. In addition, when performing IFFT, the remaining subcarriers are zero-padded. Then, a cyclic prefix (CP) of 1/16 length of the OFDM symbol is appended to prevent inter symbol interference after performing IFFT of the encrypted data and P/S conversion.

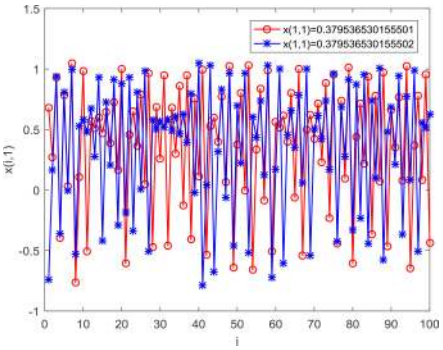


Fig. 6. Variation of the iteration states with initial value's tiny change.

The initial keys of chaotic systems are only preshared between the OLT and the legal ONU. The signal encryption is processed by MATLAB at OLT. And then, the encrypted data are loaded into an arbitrary waveform generator (AWG). The electrical signal is generated.

A continuous wave laser is used as an optical carrier. The encrypted OFDM signal is sent to a Mach–Zehnder modulator (MZM), which can convert the electrical signal into an optical signal. After transmitted over 60-km SSMF, the optical signal is finally captured by a photodiode (PD). After a series of subsequent operations, such as OFDM signal demodulation, channel estimation, spiral descrambling and DNA encoding decryption, are processed by DSP, the original data can be recovered.

4. Result and Discussions

First, the size of the key space of the system and the sensitivity of the chaotic sequence to the initial values are analyzed to guarantee the security of the proposed encryption scheme. Then, to further evaluate the reliability and feasibility of the proposed security scheme, the bit error ratio (BER) performance of encrypted 16-QAM OFDM data that are transmitted over 60-km SSMF is demonstrated and analyzed.

4.1 Security Analysis

4.1.1 Sensitivity Analysis: The size of the key space and the sensitivity to the initial values are the main elements that affect the security performance of the system. First, the chaotic characteristics of the spatially generalized Logistic system are studied. In order to guarantee that the sequences generated by chaos have satisfactory randomness, unpredictability and ergodicity, the parameters μ and ω are typically selected in the ranges of $[1.55, 2)$ and $[-0.5, 0)$, respectively.

Fig. 6 shows the variation of iteration states when the initial value changes slightly. The figure illustrates one of states of the chaotic system, i.e., $x(m, 1)$, changing initial value slightly. According to the figure, if only the 15_*th*-decimal digit of the initial value is changed, the iteration trajectory will be completely different, which indicates that the chaotic system is extremely sensitive to initial values.

4.1.2 Key Space Analysis: The size of the key space directly affects whether the system can effectively prevent eavesdropper attacks, and the larger the key space, the higher the resistance to attackers. The spatially generalized Logistic system is employed to obtain the control parameters, five states of which are used to control the DNA encoding encryption process and two states of which are used to control the spiral scrambling process. The key space of the proposed method consists of the initial values of the chaotic systems and the system parameters μ, and ω. Since the initial value $x(1, i) \quad (i = 1, 2, \ldots, 7)$ and system parameters μ and ω are the security keys, the key space can reach a size of approximately $(1 \times 10^{15})^7 \times 10^{15} \times 10^{15} = 1 \times 10^{135}$ when the accuracy of the computer reaches 10^{-15}. At the speed of the current fastest supercomputer,

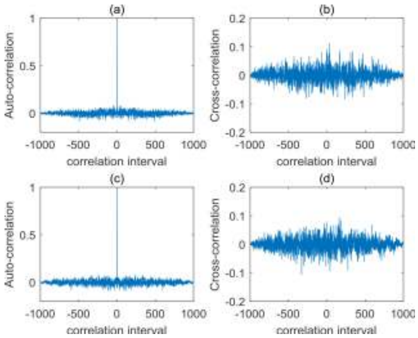


Fig. 7. Correlations of sequences iterated from states $x(m,3)$ and $x(m,4)$.

namely, Sunway TaihuLight, which is approximately $1.25 \times 10^{17} s^{-1}$, it will take at least 8×10^{117} years to obtain the correct key for the encrypted data. This huge amount of the time demonstrates that the key space is sufficiently large and has a strong resistance against brute-force attacks from illegal attackers.

In pursuit of satisfactory security performance, compared to the scheme only with DNA encoding encryption in OFDM-PON, the proposed scheme has a slightly higher time complexity due to the addition of the spiral scrambling algorithm.

However, although the chaotic DNA encoding encryption method considers the security of the transmission system and has a slightly lower time complexity, the proposed hybrid secure method, which is based on DNA encoding encryption and spiral scrambling is more effective for enhancing the physical-layer security and it can provide a larger key space for resisting malicious attacks since the controlling parameters for DNA encoding encryption and spiral scrambling are produced by the spatially generalized Logistic system. The discrete chaotic system employed in the proposed scheme reduces the complexity of generating chaotic sequences compared to schemes that use continuous chaotic systems as pseudo-random sequence generators.

4.1.3 Correlation Analysis: Fig. 7 plots the auto-correlations and cross-correlations of the generated sequences that utilize iteration states $x(m,3)$ and $x(m,4)$. And Fig. 7(a) and (c) are auto-correlation functions of sequences iterated from states $x(m,3)$ and $x(m,4)$ respectively. Fig. 7(b) shows a cross-correlation function between the sequence iterated from state $x(m,3)$ with the original initial value and the sequence generated by the iteration of state $x(m,3)$ when the initial value is slightly changed. Similarly, the cross-correlation function shown in Fig. 7(d) is obtained from state $x(m,4)$. From Fig. 7, it can be seen that the auto-correlation function is a unit pulse function and the cross-correlation function is close to zero. The generated sequences have satisfactory characteristics of auto-correlation and cross-correlation, which provides high security to the proposed physical-layer encryption method.

4.2. BER Performance Analysis

The QAM symbol matrix is divided into several blocks and inter-block scrambling is conducted. In order to determine whether the size of the block used for scrambling has an impact on the BER performance of the transmitted data, the block sizes are set to 8 × 8, 8 × 4, 4 × 8 and 4 × 4. Fig. 8 presents the BER performance curves of the encrypted OFDM signal with various block sizes. The simulation results demonstrate that the size of the block used for scrambling will affect the BER performance of the transmitted signal at the receiver. As can be seen from the figure, the BER performance of the method with the block size of 8 × 4 (mn84) has been improved by ∼0.7 dB and ∼1 dB at a BER of 10^{-3} (FEC limit) compared with the methods with block size of 8 × 8 (mn88) and 4 × 4 (mn44), respectively. The 4 × 8-block-size (mn48) scheme and the 8 × 4 scheme realize almost the same BER performance. At the same time, it cannot be ignored that the BER performance of the 4 × 4-block-size scheme also deteriorates as the signal-to-noise ratio

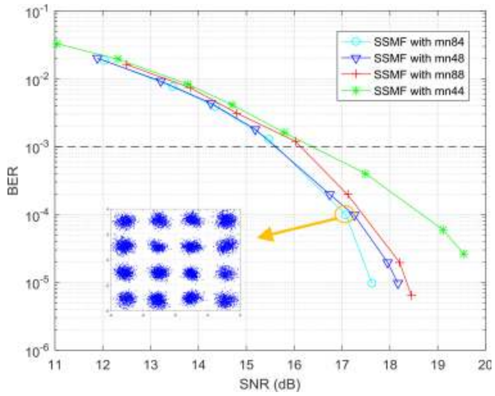


Fig. 8. BER curves with various block sizes.

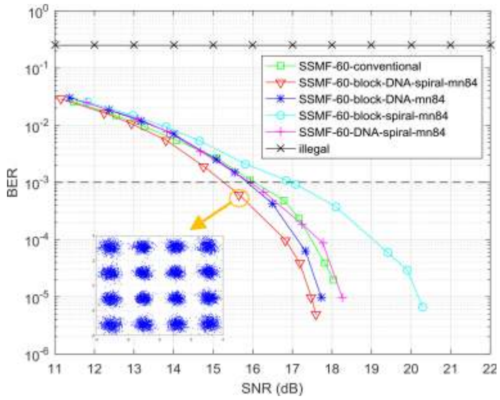


Fig. 9. BER curves of signals with various encryption methods.

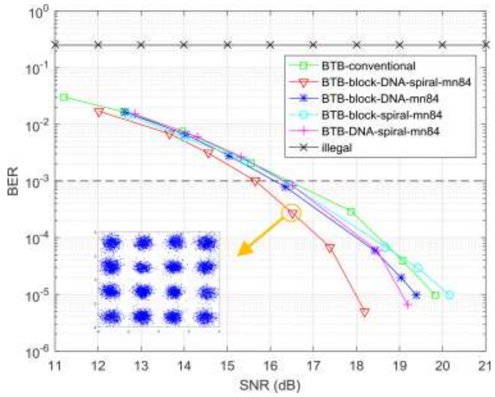


Fig. 10. BER curves of various encryption methods of BTB.

(SNR) increases. The downward trends of the BER curves of the other three schemes will be stronger, which demonstrates that they can maintain satisfactory BER performance all the time. Therefore, in the proposed scheme, in order to ensure the optimal BER performance, the block size of 8×4 is selected for scrambling.

In addition, the BER curves of various schemes in the cases of 60-km SSMF and BTB transmission have been examined, which are plotted in Figs. 9 and 10, respectively. These schemes include the conventional scheme; the proposed scheme with DNA encoding encryption, spiral scrambling and block scrambling; the scheme with DNA encoding encryption and block scrambling;

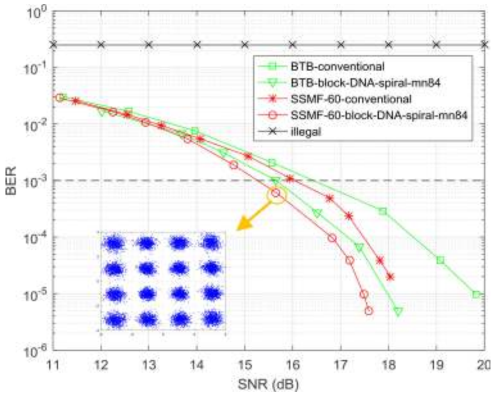


Fig. 11. BER curves of the proposed method of BTB and 60-km.

the scheme with spiral scrambling and block scrambling; and the scheme with DNA encoding encryption and spiral scrambling.

According to figures, in these two cases, a legitimate user can correctly decrypt the transmitted data; however, for an illegal user, the bit error rate is as high as 0.5 due to an incorrect key; hence, an illegal user cannot correctly decrypt the transmitted data.

It can be seen in Fig. 9 that, the BER performance of the proposed security method has been improved by ∼1 dB at a BER of 10^{-3} compared with the conventional method over 60-km SSMF transmission. Relative to the method without DNA encoding encryption, the BER performance with DNA encoding encryption can be improved by nearly 2 dB. At the same time, the spiral scrambling encryption can improve the BER performance by ∼0.75 dB at a BER of 10^{-3}, as shown by the blue and red lines. Compared with the scheme without block scrambling, the proposed method with block scrambling shows ∼0.8 dB improvement in BER performance, which means that the block scrambling contributes to the performance of the system. In summary, the methods without spiral scrambling, without DNA encoding encryption or without block scrambling exhibit worse BER performance than the proposed scheme, which can better enhance BER performance and improve system security.

Fig. 10 shows the BER curves of the various schemes in the case of BTB. The BER performance of proposed security method has been improved by ∼1 dB over the conventional method at a BER of 10^{-3}. Compared to the methods without spiral scrambling, without DNA encoding encryption or without block scrambling, the BER performance of proposed method has been improved by approximately 0.5 dB, 1 dB and 1 dB, respectively. According to the simulation results, the proposed scheme over 60-km SSMF has maintained good transmission performance.

For a clearer comparison, the BER curves for the case of BTB and 60-km SSMF transmission are plotted together in Fig. 11, in which the curve at 60-km SSMF is shown as a red line with circles and the curve at BTB is shown as a green line with triangles. BTB transmission outperforms 60-km SSMF transmission at low SNR, and the performance of 60-km SSMF will be better than BTB except in the case of illegal ONU. At the BER of 10^{-3}, the BER performance of the proposed method has been improved by approximately 0.5 dB in the case of 60-km SSMF compared to BTB. In both 60-km SSMF transmission and BTB, the proposed scheme has a better BER performance than the conventional scheme. Hence, the proposed scheme yields an improvement in terms of reliability.

Fig. 12 plots the BER curves of our proposed scheme with DNA encoding encryption and spiral scrambling and the scheme only with DNA encoding encryption by simulation [31]. According to the figure, the proposed scheme exhibits superior BER performance by approximately 1 dB compared to the previous method at the BER of 10^{-3}. This enhancement of BER performance can be attributed to the spiral scrambling and the block scrambling. In the case of BTB, a ∼0.5-dB improvement of BER performance is also realized with the proposed method. Hence, the proposed scheme can enhance both the encryption ability and the transmission performance.

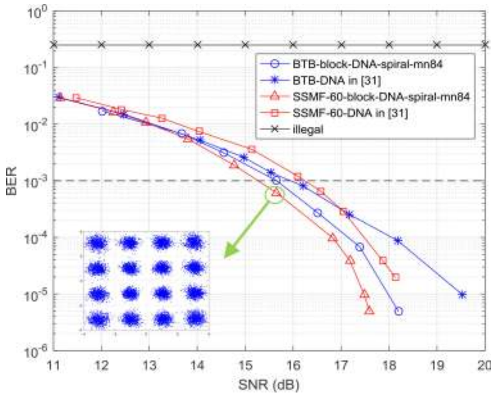


Fig. 12. BER curves of the proposed method and the method in [31].

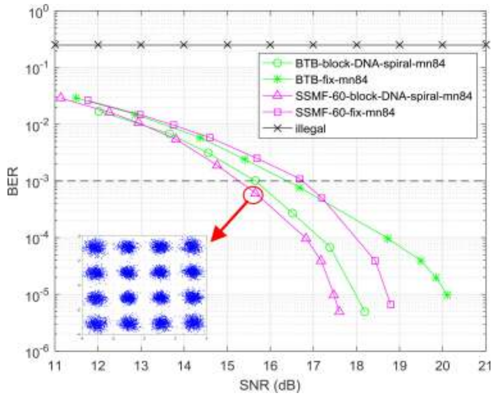


Fig. 13. BER curves of the proposed method and the method with fixed DNA encryption parameters.

In the DNA encryption process, each chaotic sequence is employed as a controlling parameter, which controls the selection of the DNA encoding rules. However, if each controlling parameter is fixed, only one of the DNA encoding rules will be used, which will reduce the system performance. Fig. 13 compares the BER performances of the proposed method and the method with fixed controlling parameters. According to the figure, the method with fixed controlling parameters exhibits an inferior BER performance of ∼1.5 dB compared to the proposed scheme with the dynamic controlling parameters over 60-km SSMF data transmission. Therefore, dynamic controlling parameters can substantially improve the transmission performance.

5. Conclusion

In this paper, a novel hybrid secure method based on improved DNA encoding encryption and spiral scrambling scheme in OFDM-PON is proposed for enhancing the physical-layer security. In the proposed scheme, improved DNA encoding encryption is employed, and block scrambling and spiral scrambling are performed. All these operations are controlled by a spatially generalized Logistic system, which can enhance the complexity of the key space and the security of the system. A key space of $\sim 1 \times 10^{135}$ can be achieved in the multi-fold encryption of the proposed encryption scheme. Comparing the proposed scheme with other schemes, the simulation results demonstrate that the proposed scheme not only has a larger key space, but can also resist illegal attacks and realizes improved BER performance over 60-km SSMF transmission. The proposed scheme is a preeminent candidate for meeting the demands of next-generation secure OFDM-PON.

References

[1] J. Zhang *et al.*, “200-Gb/s/λ PDM-PAM-4 PON with 29-dB power budget based on heterodyne coherent detection,” in *Proc. Opt. Fiber Commun.*, San Diego, USA, 2019, Paper Th3F.1.

[2] J. Zhang, “Demonstration of 100-Gb/s/λ PAM-4 TDM-PON supporting 29-dB power budget with 50-km reach using 10G-class O-band DML transmitters,” in *Proc. Opt. Fiber Commun.*, San Diego, USA, 2019, Paper Th4C.3.

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

[4] 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.

[5] M. Bi, X. Fu, X. Zhou, X. Yang, S. Xiao, and W. Hu, “Chaotic nonlinear encryption scheme for CPAs resistance and PAPR reduction in OFDM-PON,” *IEEE Photon. Technol. Lett.*, vol. 29, no. 24, pp. 2147–2150, Dec. 2017.

[6] Z. Zhao *et al.*, “Semiconductor-laser-based hybrid chaos source and its application in secure key distribution,” *Opt. Lett.*, vol. 44, no. 10, pp. 2605–2608, 2019.

[7] T. Li and J. Yorke, “Period three implies chaos,” *Amer. Math. Monthly*, vol. 82, no. 10, pp. 985–992, 1975.

[8] S. Li *et al.*, “Secure key distribution strategy in OFDM-PON by utilizing the redundancy of training symbol and digital chaos technique,” *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7201108.

[9] B. Liu, L. Zhang, X. Xin, and Y. Wang, “Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation,” *IEEE Photon. Technol. Lett.*, vol. 26, no. 2, pp. 127–130, Jan. 2014.

[10] L. Zhang, B. Liu, and X. Xin, “A novel 3D constellation-masked method for physical security in hierarchical OFDMA system,” *Opt. Express*, vol. 21, no. 13, pp. 15627–15633, Jul. 2013.

[11] A. Argyris *et al.*, “Chaos-based communications at high bit rates using commercial fibre-optic links,” *Nature*, vol. 438, no. 7066, pp. 343–346, 2005.

[12] T. Kodama *et al.*, “Secure 2.5 Gbit/s, 16-ary OCDM block-ciphering with XOR using a single multi-port en/decoder,” *J. Lightw. Technol.*, vol. 28, no. 1, pp. 181–187, 2010.

[13] A. Sultan, X. Yang, A. Hajomer, and W. Hu, “Chaotic constellation mapping for physical-layer data encryption in OFDM-PON,” *IEEE Photon. Technol. Lett.*, vol. 30, no. 4, pp. 339–342, Feb. 2018.

[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] 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.

[16] 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.

[17] 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.

[18] A. 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, Jun. 2017.

[19] J. Xiao *et al.*, “Hadamard transform combined with companding transform technique for PAPR reduction in an optical direct-detection OFDM system,” *J. Opt. Commun. Netw.*, vol. 4, no. 10, pp. 709–713, Oct. 2012.

[20] Y. Xiao, M. Chen, F. Li, J. Tang, Y. Liu, and L. Chen, “PAPR reduction based on chaos combined with SLM technique in optical OFDM IM/DD system,” *Opt. Fiber. Technol.*, vol. 21, pp. 81–86, Jan. 2015.

[21] T. Wu *et al.*, “Security enhancement for OFDM-PON using Brownian motion and chaos in cell,” *Opt. Express*, vol. 26, no. 18, pp. 22857–22865, Sep. 2018.

[22] X. Hu, X. Yang, Z. Shen, H. He, W. Hu, and C. Bai, “Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON,” *IEEE Photon. Technol. Lett.*, vol. 27, no. 23, pp. 2429–2432, Dec. 2015.

[23] T. Wu, C. Zhang, H. Wei, and K. Qiu, “PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM,” *Opt. Express*, vol. 27, no. 20, pp. 27946–27961, Sep. 2019.

[24] C. Zhang, W. Zhang, X. He, C. Chen, H. Zhang, and K. Qiu, “Physically secured optical OFDM-PON by employing chaotic pseudorandom RF subcarriers,” *IEEE Photon. J.*, vol. 9, no. 5, Oct. 2017, Art. no. 7204408.

[25] W. Zhang, C. Zhang, C. Chen, H. Zhang, W. Jin, and K. Qiu, “Hybrid chaotic confusion and diffusion for physical layer security in OFDM-PON,” *IEEE Photon. J.*, vol. 9, no. 2, Apr. 2017, Art. no. 7201010.

[26] S. Li *et al.*, “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.

[27] Y. Xiao *et al.*, “Time-frequency domain encryption with SLM scheme for physical-layer security in an OFDM-PON system,” *J. Opt. Commun. Netw.*, vol. 10, no. 1, pp. 46–51, Jan. 2018.

[28] B. Liu, L. Zhang, X. Xin, and N. Liu, “Piecewise chaotic permutation method for physical layer security in OFDM-PON,” *IEEE Photon. Technol. Lett.*, vol. 28, no. 21, pp. 2359–2362, Nov. 2016.

[29] Y. Xiao, J. Cao, Z. Wang, C. Long, Y. Liu, and J. He, “Polar coded optical OFDM system with chaotic encryption for physical-layer security,” *Opt. Commun.*, vol. 433, pp. 231–235, Feb. 2019.

[30] X. Zhang, Z. Zhou, and Y. Niu, “An image encryption method based on the feistel network and dynamic DNA encoding,” *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 3901014.

[31] C. Zhang, W. I. Zhang, C. Chen, X. He, and K. Qiu, “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.

[32] G. Chen and S. T. Liu, “On generalized synchronization of spatial chaos,” *Chaos Solitons Fractals*, vol. 15, no. 2, pp. 311–318, 2003.