IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 22, 2020, accepted January 18, 2021, date of publication January 25, 2021, date of current version February 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3054380

Multilayer Dynamic Encryption for Security OFDM-PON Using DNA-Reconstructed Chaotic Sequences Under Cryptanalysis

MENGWEI CUI[1], CHONGFU ZHANG[1,2], (Senior Member, IEEE), YUHANG CHEN[1], ZHI ZHANG[1], TINGWEI WU[1], AND HEPING WEN[1,2]

[1]School of Information and Communication Engineering, Zhongshan Institute, University of Electronic Science and Technology of China, Chengdu 611731, China

[2]School of Electronic Information, University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China

Corresponding author: Chongfu Zhang (cfzhang@uestc.edu.cn)

This work was supported in part by the National Science Foundation of China under Grant 62071088 and Grant 61571092, in part by the Project for Innovation Team of Guangdong University under Grant 2018KCXTD033, in part by the Project for Zhongshan Social Public Welfare Science and Technology under Grant 2019B2007, and in part by the Research Project for Talent of UESTC Zhongshan Institute under Grant 418YKQN07.

ABSTRACT In this paper, a multilayer dynamic encryption scheme using deoxyribonucleic acid reconstructed chaotic sequences (DNA-RCS) under cryptanalysis is firstly proposed, which aims at enhancing the security of orthogonal frequency division multiplexing passive optical network (OFDM-PON). We adopt DNA coding to reconstruct chaotic sequences, the selected coding rules and the number of chaotic sequence blocks divided are then random, the randomness and security of encryption sequences are improved. The transmitted signal is encrypted in two layers. The first layer is hybrid chaotic permutation and diffusion. Each symbol can be encrypted by the combination of a single non-repetitive permutation and plaintext-related diffusion. It makes encryption not only depend on the chaotic sequences but also relate to the order of permutation. The second layer is a dynamic Josephus permutation. By taking the unit as the permutation object, the scrambling efficiency is increased. Also, the counting period is randomly selected, which can enhance the security of the system. The number of tests needed to break a secure transmission for an attacker can reach up to 3.096×10^{106}. An encryption signal with 22.06Gb/s is successfully demonstrated over a 25-km standard single-mode fiber (SSMF) and a back-to-back (BTB) system. It is proved that the proposed scheme does not degrade the system performance and can effectively resist various attacks by the performance analysis model based on cryptanalysis.

INDEX TERMS Cryptanalysis, DNA-reconstructed chaotic sequences, multilayer dynamic encryption, OFDM-PON.

I. INTRODUCTION

Orthogonal frequency division multiplexing passive optical network (OFDM-PON), as the optimal scheme for next-generation access network, can provide users with large bandwidth and low-cost services due to its advantages such as flexible resource allocation, high spectrum efficiency, and strong robustness against fiber dispersion [1], [2]. However, with the continuous growth of users, there are plenty of frequent service interactions between optical network units (ONUs) and optical line terminal (OLT) [3]. The downlink broadcast communication data in OFDM-PON is vulnerable to malicious eavesdropping and attack by illegal ONUs [4], [5]. Therefore, the security of OFDM-PON has attracted wide attention by more and more scholars.

To solve this problem, many studies have been proposed. Among them, physical layer chaotic communication to enhance the security of OFDM-PON has become the main solution. A new method of masking OFDM subcarriers and controlling the fractional order of the fractional Fourier transform can enhance physical layer security [6]. A Rubik's Cube (RC) transformation algorithm is used to generate a key stream for symbol substitution [7]. The reliability of the physical layer is improved by scrambling subcarriers [8]–[10]. Double-chaos is used for floating probability shaping (PS). This scheme achieves high sensitivity and security [11].

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

The optimal frame transmission technology based on IQ encryption can not only enhance security but also reduce PAPR and solve the problem of low transmission rate [12]. A super OFDM frame is generated by chaotic frame interleaving, and the spectral efficiency is improved by the chaotic active constellation extension [13]. A 2-D logistic adjusted sine map is used for optimal block dividing and dynamic key distribution to realize PAPR reduction and security improvement in OFDM-PON [14]. A chaotic discrete Hartley transform is used to enhance the physical layer security after independent row/column permutations [15]. This scheme has lower computational complexity and higher spectral efficiency due to no additional sideband information. Besides, some scholars proposed the combination of chaotic encryption and code. DNA code and DNA extension code are used to enhance the complexity and randomness of the encryption sequences [16], [17]. Also, the subcarrier rotation based on turbo code is used to realize security communication [18]. But these methods mainly use encoding for bit sequence encryption. The encryption process is a little simple.

At present, there are also many multilevel encryption schemes. The symbol substitution and interleave are adopted for encryption [19]. Dynamic radius and phase offsets are added into the constellation to achieve multifold security data encryption [20]. A 7-D hyperchaos is adopted to implement two-layer encryption, where Walsh-Hadamard and discrete cosine transform are used to effectively reduce the computational complexity and increase the key space [21]. A security enhancement scheme combining improved DNA coding at the bit-level and matrix scrambling at the symbol-level is proposed to obtain a larger key space and ensure the security of the physical layer [22]. A two-level encryption method of multi-scroll chaotic systems for I/Q encryption and column permutation is proposed [23]. The quadrature amplitude modulation (QAM) matrix is divided and encrypted by different algorithms according to the order of the submatrix [24]. A noise-like constellation or subcarriers are scrambled in the time and frequency domains [25], [26]. The transmission image is encrypted by the 4-D hyper-Arnold map at the upper layer. Then the chaotic scrambling sequence based on the Arnold map is used to encrypt the image again at the physical layer, which further enhances the security of the transmitted image [27]. However, most of the above encryption schemes to improve security are based on symbols or bit sequences alone. The permutation objects are relatively single.

Besides, with the improvement of computing, many cryptographic systems are facing the threat of being cracked. The authors pointed out that chaotic encryption methods based on permutation still have security risks [28], [29], which are difficult to resist chosen plaintext/ciphertext attacks (CPA/CCA). The authors proved that the keys of some chaotic digital image encryption schemes have security defects [30], [31]. They can be completely cracked due to the lack of effective cryptanalysis. At present, only some of the encryption methods consider the security of OFDM-PON under a plaintext attack. For example, a 4-D hyperchaotic system is used to construct nonlinear substitution boxes (S-boxes) [32]. A cyclic XOR operation is performed to generate nonlinear transformation bit data by the S-boxes. This scheme can improve resistance to CPAs. Dynamic codebooks are generated using the randomness of chaotic keys and input data to achieve chaotic permutation and polarity reversal of subcarriers [33], but it is only proved by Monte Carlo simulation that it can resist known plaintext attacks (KPAs) and CPAs. Therefore, it is necessary to evaluate the provable security of physical layer encryption schemes in OFDM-PON under cryptanalysis.

In this paper, a multilayer dynamic encryption scheme for security OFDM-PON using DNA-reconstructed chaotic sequences (DNA-RCS) under cryptanalysis is proposed. First, the chaotic sequences are reconstructed by DNA coding, which increases the randomness of the encryption sequences and solves the problems of low security of low-dimensional chaos and complex realization of high-dimensional chaos. Then, the DNA-RCS is used for data encryption in two layers. The first layer is hybrid chaotic permutation and diffusion. The second layer is a dynamic Josephus permutation. The two-layer encryption achieves non-repetitive permutation from symbols to units and ensures the high-security encryption of the system. Also, the ciphertext enhances the ability to resist the attackers by the plaintext-related diffusion. The proposed scheme is proved by the cryptanalysis model that it is a provable security access network scheme.

II. PRINCIPLE

The schematic diagram of the proposed multilayer dynamic encryption scheme using DNA-RCS is shown in Fig. 1. At the OLT, a pseudo-random binary sequence (PRBS) is used as input data. After serial-to-parallel (S/P), QAM modulation, and subcarrier allocation, a plane matrix $P = F \times N$ can be obtained. F represents the number of subcarriers, and N represents the number of QAM symbols on each subcarrier. The matrix P is encrypted with hybrid chaotic permutation and diffusion, and dynamic Josephus permutation based on the DNA-RCS. Then, the signal after encryption is converted from the frequency domain to the time domain by IFFT. The operations of inserting cyclic prefix (CP) and parallel-to-serial (P/S) are conducted. Finally, the signal can be transmitted to the ONU.

A. DNA-RECONSTRUCTED CHAOTIC SEQUENCES

A DNA sequence contains four bases: adenine (A), guanine (G), thymine (T), and cytosine (C). According to the principle of base complementation of DNA, two deoxynucleotide chains are opposite complementary and form stable combinations through hydrogen bonds between bases, in which A and T are complementary pairs, and C and G are complementary pairs [16]. Each base is usually encoded by two binary bits consisting of "0" and "1", so $4 \times 3 \times 2 \times 1 = 24$ coding rules can be obtained. However, only 8 coding rules can meet the

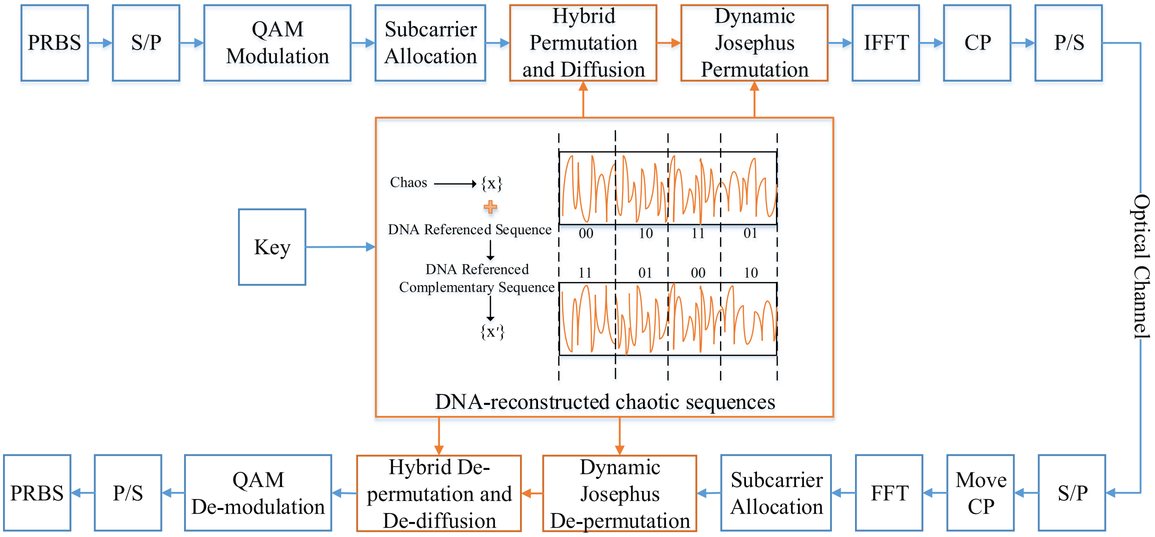
PRBS
S/P
QAM Modulation
Subcarrier Allocation
Hybrid Permutation and Diffusion
Dynamic Josephus Permutation
IFFT
CP
P/S
Key
Chaos → {x}
DNA Referenced Sequence
DNA Referenced Complementary Sequence
{x'}
00 10 11 01
11 01 00 10
DNA-reconstructed chaotic sequences
Optical Channel
S/P
Move CP
FFT
Subcarrier Allocation
Dynamic Josephus De-permutation
Hybrid De-permutation and De-diffusion
QAM De-modulation
P/S
PRBS

FIGURE 1. The schematic diagram of the proposed multilayer dynamic encryption scheme using DNA-RCS.

TABLE 1. DNA encoding and decoding rules.

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

principle of base complementation requirements, as shown in Table 1.

In this paper, 1-D logical chaos is employed as the basis for DNA-RCS, which is written as

$$x_{i+1} = \mu x_i\left(1 - x_i\right) \tag{1}$$

where x_i ($x_i \in [0, 1]$) represents the result of the i-th iteration, and μ represents the bifurcation parameter. When $\mu \in (3.57, 4)$, 1-D logical chaotic map shows a good chaotic state [24].

DNA referenced sequence is obtained as

$$T_x = mod\left(Extract\left(x_i, a, b, c\right), Q\right)/Q \tag{2}$$

where $Extract$ (x_i, a, b, c) returns an integer composed of the a-th, b-th, and c-th digits in the decimal part of $\{x\}$, mod (s, t) returns the remainder of s divided by t, and Q represents the maximum of QAM symbols on each subcarrier. In this scheme, Q is set to 200. Then, T_x is converted into a binary sequence $\{T\}$ with m bits reserved. $\{T\}$ is used as a referenced sequence for DNA coding. The DNA referenced complementary sequence $\{T'\}$ can be obtained by encoding every two bits of $\{T\}$. The chaotic sequence $\{x\}$ is reconstructed by $\{T'\}$ as follows:

$$(q-1)\times\left({}^{N}\!/_{M}\right) < n \le q\times\left({}^{N}\!/_{M}\right),\quad q = 1, 2, \ldots, M \tag{3}$$

$$M = m/2 \tag{4}$$

$$N = kM,\quad k = 1, 2, 3\ldots \tag{5}$$

$$x_q' = \begin{cases} x_q, & T_t'T_f' = 00 \\ x_q\left({}^{N}\!/_{M} - \alpha\right), & T_t'T_f' = 01 \\ x_q\left({}^{N}\!/_{M} - \alpha\right), & T_t'T_f' = 10 \\ (-1)\times x_q, & T_t'T_f' = 11 \end{cases} \tag{6}$$

where m is the length of the DNA referenced complementary sequence $\{T'\}$, n ($n = 1, 2, \ldots, N$) is the length of the chaotic sequence $\{x\}$, M ($M \in Z$) represents the number of blocks divided in the chaotic sequence $\{x\}$, and $\alpha(0 < \alpha < N/M)$ is the number of moving bits of a chaotic sequence block, which is set to 10. $\{x_q\}$ represents a chaotic sequence block, and $\{x_q'\}$ represents a reconstructed chaotic sequence block. Each block is controlled by two bits of $\{T'\}$. If $T_t'T_f' = 00$, the waveform of the original chaotic sequence block remains unchanged. If $T_t'T_f' = 01$, the waveform is shifted circularly to the right by α. If $T_t'T_f' = 10$, the waveform is shifted circularly to the left by α. If $T_t'T_f' = 11$, the waveform flips vertically. Finally, the DNA-RCS $\{x'\}$ is obtained by splicing the transformed chaotic sequence blocks according to the order of divided blocks.

B. THE FIRST LAYER HYBRID CHAOTIC PERMUTATION AND DIFFUSION

The DNA-RCS is used to carry out the first layer hybrid chaotic permutation and diffusion encryption on the matrix P. This process performs single non-repetitive encryption on the rows and columns of the matrix P so that each symbol can be scrambled. Moreover, the interaction between permutation and diffusion increases the difficulty of being attacked separately. The specific steps are as follows:

Step 1: The DNA-RCS $\{x'\}$, $\{y'\}$, $\{z'\}$, $\{w'\}$ are generated.

Step 2: $\varphi \in [0, 1]$ is divided into F intervals. Each interval is numbered in ascending order from 1 to F. The sequence $\{x_1'\}$ with length F is arbitrarily chosen from the

DNA-RCS $\{x'\}$. The values in the $\{x'_1\}$ are judged to be mapped in the F_i-th interval. Next, the intervals are reordered according to the mapping order to generate a new row index vector I_x. Note that the mapping of the random number in the same interval remains only one, and the intervals that are not judged by $\{x'_1\}$ are arranged at the end in ascending order of the original index. Then, the row index of the matrix P is

$$I_x = exchange\,(F_1, F_2, \ldots F_i, \ldots F_F) \tag{7}$$

where *exchange* $(\cdot)$ returns the row index reordered by the mapping, and i $(i = 1, 2, \cdots, F)$ is the initial index of the row.

Step 3: The DNA-RCS $\{y'\}$ is binarized to obtain a uniformly distributed digital chaotic sequence as

$$y''_i = \begin{cases} 0, & y'_i \le 0.5 \\ 1, & y'_i > 0.5 \end{cases} \quad (1 \le i \le n) \tag{8}$$

After that, the sequence $\{y''_1\}$ with length N is arbitrarily chosen from the $\{y''\}$, which corresponds to the row symbols in the matrix P. The symbols corresponding to "1" are diffused.

$$L'_1 = L_1 \tag{9}$$

$$L'_j = L_j \oplus L'_{j-1} \tag{10}$$

where L_j $(j \in [1, N])$ is the symbol corresponding to "1" in the row, and L'_j $(j \in [1, N])$ is the row symbol after diffusion. The operation "$\oplus$" performs the bit-XOR between two symbols. When the diffusion of a row is completed, the $\{y''_1\}$ is transformed as

$$y''_2 = rcycle\left(y''_1, d\right) \tag{11}$$

where *rcycle* $(\cdot)$ returns the new sequence $\{y''_2\}$ after $\{y''_1\}$ is shifted circularly to the right by d. In this scheme, d is set to 1. Therefore, the row diffusion of the matrix is related not only to the DNA-RCS but also to the order of the row permutation in the second step. An example can briefly show the hybrid chaotic permutation and diffusion for row symbols in Fig. 2.

Step 4: The column permutation is performed using the DNA-RCS $\{z'\}$ as step 2. The column index of the matrix P is

$$I_y = exchange\left(N_1, N_2, \ldots N_j, \ldots N_N\right) \tag{12}$$

where j $(j = 1, 2, \cdots, N)$ is the initial index of the column.

Step 5: The column diffusion is performed by using the DNA-RCS $\{w'\}$ as step 3, which is expressed as

$$R'_1 = R_1 \tag{13}$$

$$R'_i = R_i \oplus R'_{i-1} \tag{14}$$

$$w''_2 = rcycle\left(w''_1, d\right) \tag{15}$$

where R_i $(i \in [1, F])$ is the symbol corresponding to "1" in the column, and R'_i $(i \in [1, F])$ is the column symbol after diffusion.

After the first layer hybrid chaotic permutation and diffusion, the matrix P is converted into the encryption matrix P_1.

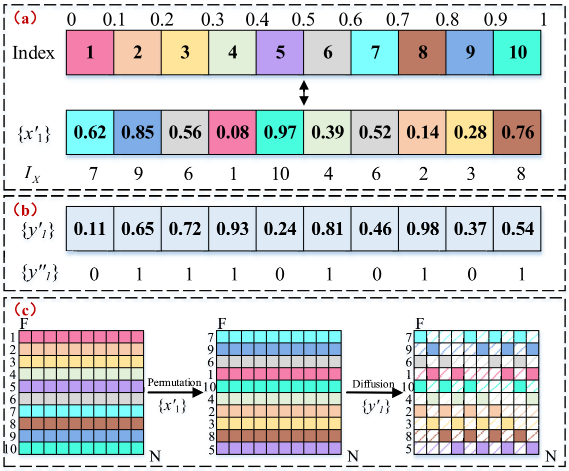

FIGURE 2. The example of hybrid chaotic permutation and diffusion for row symbols. (a) Random mapping permutation; (b) binarization; (c) hybrid chaotic permutation and diffusion.

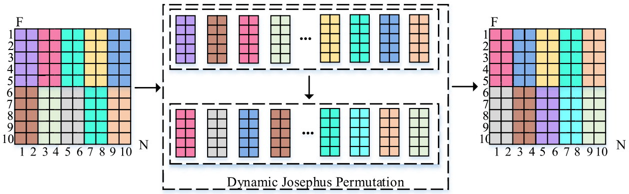

FIGURE 3. The example of dynamic Josephus permutation.

C. THE SECOND LAYER DYNAMIC JOSEPHUS PERMUTATION

The Josephus traversal sequence [34] is

$$sq = JosephusTraverse\,(K, s, t) \tag{16}$$

where K represents the length of the original sequence, $s \in [1, K]$ represents the starting position of the traversal, and t is the counting period. Since the counting period is fixed in the process of Josephus traversal, the randomness of the encryption results can be reduced. Therefore, the DNA-RCS is used to update the counting period of each round in this scheme to realize dynamic Josephus traversal. The matrix $P_1 = F \times N$ is divided into units, as shown in Fig. 3. The number of permutation objects is reduced, and the scrambling efficiency is improved. The specific steps are as follows:

Step 1: To facilitate permutation, we set the size of each unit to be the same. This step also applies to units of different sizes. We assume that the number of subcarriers in each unit after division is f, and the number of symbols on each subcarrier is n, which is expressed as

$$f = g\,(mod\,(F, g) = 0)\,, \quad g = 1, 2, \ldots, F \tag{17}$$

$$n = h\,(mod\,(N, h) = 0)\,, \quad h = 1, 2, \ldots, N \tag{18}$$

After division, the number of the subcarrier units is $N_{car} = F/f$, and the number of the symbol units is $N_{sym} = N/n$.

Step 2: The DNA-RCS $\{\gamma'\}$ is generated to select the counting period of each round of dynamic

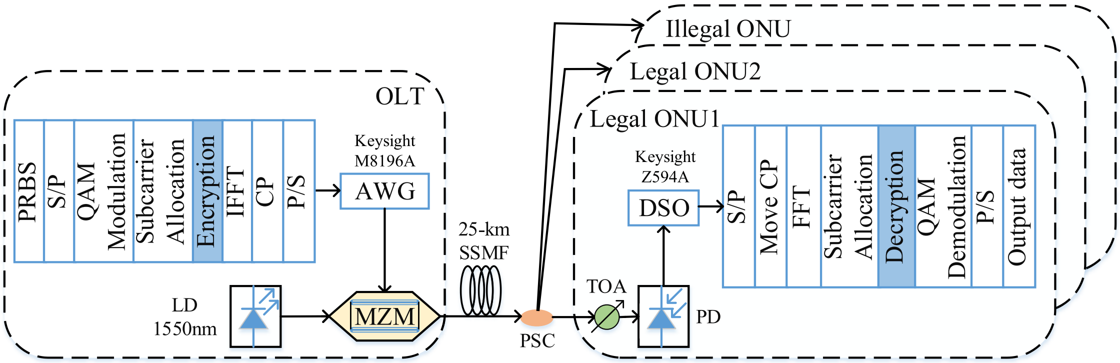

FIGURE 4. The experiment setup of the multilayer dynamic encryption scheme using DNA-RCS in OFDM-PON. (AWG: arbitrary waveform generator; LD: laser diode; MZM: Mach-Zehnder modulator; SSMF: standard single-mode fiber; PSC: passive splitter couple; TOA: tunable optical attenuator; PD: photodetector; OLT: optical line terminal; ONU: optical network unit).

Josephus permutation.

$$t = Extract\left(\gamma_i', e\right) \tag{19}$$

where $Extract\,(\gamma_i', e)$ returns the e-th digit in the decimal part of $\{\gamma'\}$.

Step 3: According to the column priority, the divided matrix $P_{Ncar\times Nsym}$ is transformed into a 1-D unit sequence of length $N_{car}\times N_{sym}$. The dynamic Josephus permutation is implemented by referring to (16). Then, the generated new unit sequence is rearranged into an encryption matrix with a size of $N_{car}\times N_{sym}$. Therefore, the matrix P_1 is converted to the encryption matrix P_2 for transmission.

III. EXPERIMENT SETUP

Fig. 4 shows the experiment setup of the proposed multilayer dynamic encryption scheme using DNA-RCS in OFDM-PON. At the OLT, the encrypted OFDM signal is generated offline by MATLAB. The length of IFFT is 256, of which the number of subcarriers to carry encrypted data is 120, and the number of symbols on each subcarrier is 200. To ensure the generation of real value signals, a data frame with a Hermitian symmetric structure is used, and the corresponding complex conjugate data is loaded on another 120 subcarriers. The length of the CP is 1/16 of the length of IFFT. We use an arbitrary waveform generator (AWG, Keysight M8196A) with a sampling rate of 12.5 GSa/s to complete a digital-to-analog conversion (DAC). A laser diode (LD) with a wavelength of 1550 nm and an output power of 14.60 dBm is applied as the optical source. Mach-Zehnder modulator (MZM) with a bandwidth of 10GHz is used for intensity modulation. The light signal is transmitted through 25-km SSMF. At the ONU, a tunable optical attenuator (TOA) is used to control the received optical power. After the light signal has been detected by a photodetector (PD) with a bandwidth of 10GHz, a digital storage oscilloscope (DSO Keysight Z594A) with a sampling rate of 25 GSa/s is used as an analog-to-digital-converter (ADC) to record it. The signal demodulation and decryption processes are also executed offline by MATLAB.

IV. RESULTS AND DISCUSSIONS

The quantitative evaluation of access network performance under cryptanalysis is a crucial reference index for evaluating encryption schemes. The performance analysis model of provable security access network encryption schemes is shown in Fig. 5. For the chaotic system and permutation mechanism adopted by the encryption schemes, the effect verification includes two aspects: security performance and communication performance. According to the attack methods, key sensitivity, and randomness of chaotic sequences in the cryptanalysis theory, the security of the system can be analyzed. According to the evaluation model of the access network communication performance, specific analysis methods and evaluation indexes are given. Based on the above results, the impact of different encryption parameters on the performance of the access network is quantitatively compared, and the validity of the security encryption schemes can be proved under cryptanalysis. The proposed scheme is analyzed and discussed based on the model as follows.

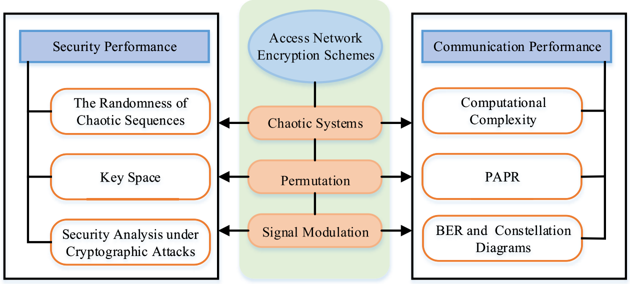
Security Performance
The Randomness of Chaotic Sequences
Key Space
Security Analysis under Cryptographic Attacks
Access Network Encryption Schemes
Chaotic Systems
Permutation
Signal Modulation
Communication Performance
Computational Complexity
PAPR
BER and Constellation Diagrams

FIGURE 5. The performance analysis model of provable security access network encryption schemes.

The chaotic initial values $[x_0, y_0, z_0, w_0, \gamma_0, \mu]$, and the number of divided blocks M of DNA-RCS are saved as a security key. We set $[x_0, y_0, z_0, w_0, \gamma_0, \mu]$ as [0.625698741145396,0.755098003973841,.598632578521655,0.425685632554689,0.356987451265859,4], and set $M = 4$.

First, we assess the sensitivity of the used encryption sequences. When the chaotic initial values x_0, μ have a tiny difference of 10^{-15}, the sensitivity of $\{x'\}$ is shown in Fig. 6(a) and (b). When $\mu = 4$, $x_0 = 0.625698741145396$, M is equal to 4 and 5, respectively, the sensitivity of $\{x'\}$ is shown in Fig. 6(c). As we can see, the trajectories are entirely different when a chaotic initial value or the number of chaotic sequence blocks is different. Therefore, when

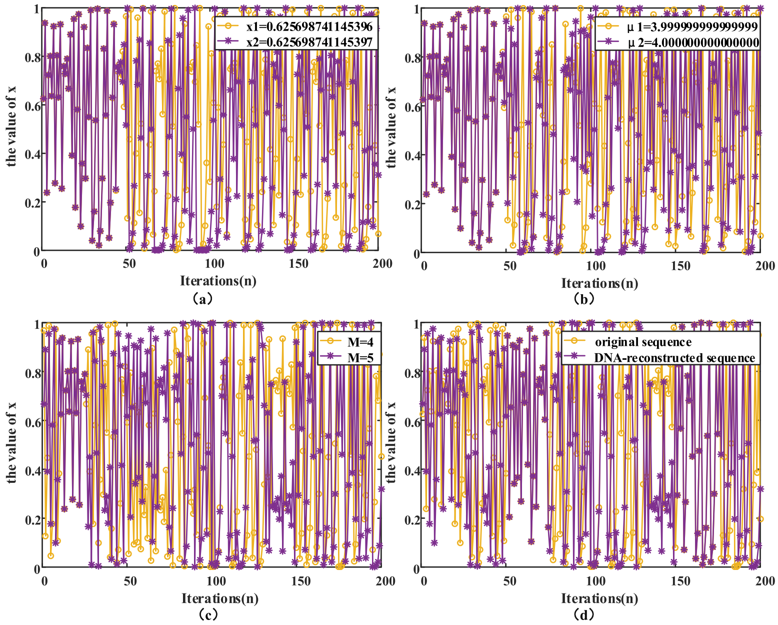

FIGURE 6. The sensitivity of {x'}. (a) The value of x_0 differs by 10^{-15}; (b) the value of μ differs by 10^{-15}; (c) the valve of M differs by 1; (d) the comparison between the original chaotic sequence and the DNA-RCS.

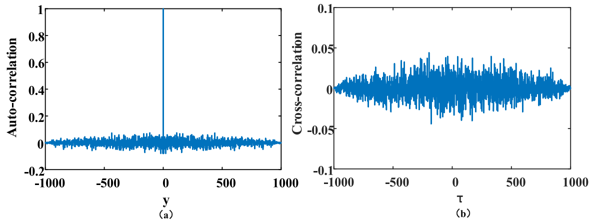

FIGURE 7. (a) The autocorrelation and (b) the cross-correlation of the DNA-RCS.

TABLE 2. The key space comparisons.

Schemes	Key space
The proposed scheme	$\sim 10^{91}$
Fractional Fourier Transform Techniques [6]	$\sim 10^{50}$
DNA extension code [17]	$\sim 10^{91}$
Hybrid chaotic confusion and diffusion [19]	$\sim 10^{60}$
7-D hyperchaos IQ [21]	$\sim 10^{253}$
Multi-scrolls system encryption [23]	$\sim 10^{56}$
Chaotic multilevel separated encryption [24]	$\sim 10^{72}$
Noise-like constellation [25]	$\sim 10^{162}$

the key is slightly changed, the ciphertext obtained will be greatly different by using different DNA-RCS to encrypt the same data. The sensitivity of the proposed scheme is high. It can effectively resist differential attacks. Fig. 6(d) shows the comparison between the original chaotic sequence and the DNA-RCS when $x_0 = 0.625698741145396$, $\mu = 4$, $M = 4$, and DNA coding in the case of rule 1. We can see that the two trajectories are noncoincidence. Since an illegal ONU does not know the specific implementation rules adopted by the DNA-RCS, the correct data information cannot be recovered even if the security key is obtained. Fig. 7 shows the autocorrelation and cross-correlation of the DNA-RCS, which displays good randomness of DNA-RCS. Therefore, compared with encryption sequences directly generated by chaos [17], [19], [24], [26], using DNA-RCS improves the randomness of chaotic sequences and the ability to resist illegal attackers.

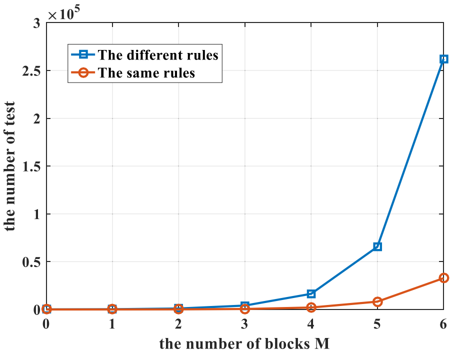

FIGURE 8. The number of tests needed to break a secure transmission.

TABLE 3. The computational complexity of the proposed scheme.

	DNA-RCS	Hybrid chaotic permutation and diffusion	Dynamic Josephus permutation	Total number
Addition	N	0	0	N
Multiplication	$6N$	$2N$	0	$8N$
Others	$3N$	$4N$	$3N$	$10N$
Total number	$10N$	$6N$	$3N$	$19N$

Second, we calculate the size of the key space. The key space provided by the chaotic sequences is (4-3.57) $\times 10^{15} \times (1 \times 10^{15})^5 = 4.3 \times 10^{89}$. To avoid continuous 0 in the DNA referenced sequence, the maximum of m is set to 50, so the

TABLE 4. **The comparisons between the proposed scheme and other multilayer encryption schemes.**

	The proposed scheme	Hybrid chaotic confusion and diffusion [19]	7-D hyper chaos IQ [21]	Chaotic multilevel separated encryption [24]	Noise-like constellation [25]	DNA extension code [17]
Addition	N	$2N$	$58.5N$	$5N$	$16N$	$3N$
Multiplication	$8N$	$6N$	$53.75N$	$10N$	$19N$	$6N$
Others	$10N$	$(N*\log_2 N)/2+3N$	$8N$	$7N$	$11N$	$5N$
Total number	$19N$	$(N*\log_2 N)/2+11N$	$120.25N$	$22N$	$46N$	$14N$

TABLE 5. **The comparisons between DNA-RCS and other chaotic systems.**

	DNA-RCS	Double chaos (2D-LASM+ 4D) [14]	LSS+LTS+TSS [17]	7D chaos [21]	4D chaos [22]	1D logistic chaos [24]	Chen's Attractor [36]
Addition	N	$10N$	$9N$	$221N$	$6N$	$1N$	$41N$
Multiplication	$6N$	$16N$	$15N$	$118N$	$8N$	$2N$	$38N$
Others	$3N$	$2N$	$3N$	$4N$	0	0	0
Total number	$10N$	$28N$	$27N$	$343N$	$14N$	$3N$	$79N$

maximum number of blocks M in this scheme is 25. The total key space is $4.3 \times 10^{89} \times 25 = 1.075 \times 10^{91}$. The key space comparisons of this proposed scheme and other encryption schemes are shown in Table 2. We can see that although the key space of this scheme is not the largest, it is sufficient to resist brute-force attacks [35]. For an illegal ONU, the number of tests needed to break a secure transmission is $(\text{A}(8,1))^2 \times 4^M$, as shown in Fig. 8. With the increase of M, the number of tests increases exponentially. If an illegal ONU only knows the encrypted OFDM symbols, when M is maximum, and DNA encoding and decoding use different rules, the total number of tests required is $4.3 \times 10^{89} \times (\text{A}(8, 1))^2 \times 4^{25} = 3.096 \times 10^{106}$ to obtain the decrypted OFDM symbol. It can be seen that the proposed scheme can resist ciphertext-only attacks. The ciphertext generated in the proposed scheme is not only related to the plaintext at this time but also related to the previous plaintext. Also, the correlation between encryption permutations is weak, and the sensitivity of the used encryption sequences is high. Therefore, it is impossible to decrypt the next valid plaintext through a known plaintext-ciphertext pair for attackers, which indicates that the proposed scheme can resist known/chosen plaintext attacks.

Third, the computational complexity of the proposed scheme comes from three processes: DNA-RCS, hybrid chaotic permutation and diffusion, and dynamic Josephus permutation. It is shown in Table 3. We use N to represent the length of the input data and assume that the length of the data transmitted is the same. The comparisons of computational complexity between the proposed scheme and other multilayer encryption schemes are shown in Table 4. To further study the performance of the used chaotic system, the comparisons between DNA-RCS and other chaotic systems are shown in Table 5. From the above results, we can see that the computational complexity of this scheme is slightly higher than that of the single-layer encryption algorithm, but compared with some other multilayer encryption schemes, the complexity of this scheme is not very high. The scrambling from symbols to units increases the difficulty of cracking the ciphertext for attacks. Besides, compared with other high-dimensional chaotic systems, the DNA-RCS used in this scheme has low computational complexity, although their computational complexities are a little higher than 1-D logistic map. Therefore, the chaotic system used in this scheme can provide high security and increase the randomness of the encryption sequences at low complexity.

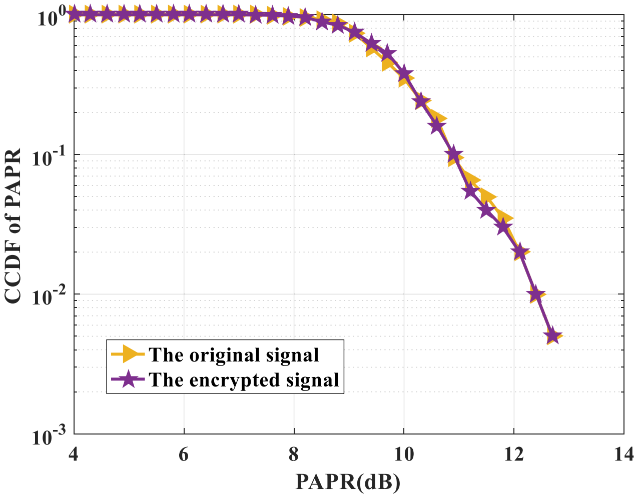

FIGURE 9. **PAPRs of the original signal and the encrypted signal.**

Fourth, we simulate the complementary cumulative distribution function (CCDF) of the peak to average power ratio (PAPR), as shown in Fig. 9. The two CCDF curves are basically overlapped, which indicates that the proposed scheme does not deteriorate the PAPR performance.

Finally, we compare the BER performance of two legal ONUs and an illegal ONU under different received optical power, as shown in Fig. 10. The BER trajectories of encrypted signals and unencrypted signals for the legal ONUs are basically coincident, indicating that the communication system using this encryption scheme has a similar performance to the standard OFDM-PON system. The received optical power

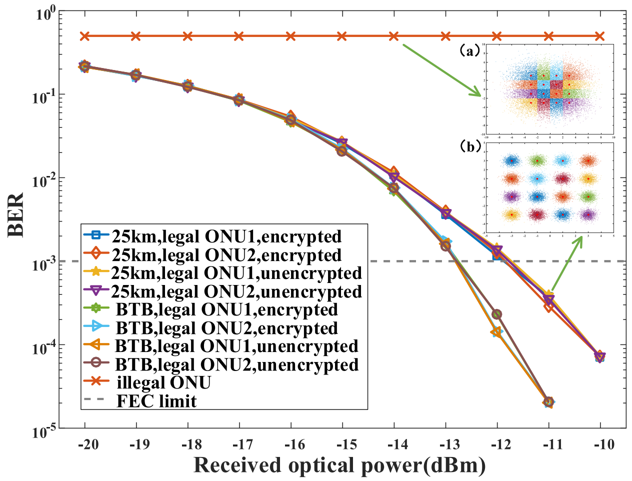

FIGURE 10. The BER performance of two legal ONUs and an illegal ONU under different received optical power.

of signals transmitted through the 25-km SSMF increases by approximately 1dBm compared with that of signals transmitted through the BTB system (BER@10^{-3}). It is mainly the influence of fiber dispersion and loss. The BER of the illegal ONU is always around 0.5. As shown in the insert (a) of Fig. 10, the illegal ONU cannot obtain any useful information from the encrypted OFDM signal due to the lack of a correct security key. The insert (b) of Fig. 10 is the constellation diagram of a 25-km SSMF transmission signal received by a legal ONU. These results indicate that the proposed scheme ensures the security of the communication system.

V. CONCLUSION

Multilayer dynamic encryption using DNA-reconstructed chaotic sequences under cryptanalysis has been proposed. An encryption signal with 22.06Gb/s was successfully transmitted over a 25-km SSMF and a BTB system, which proves that this scheme can improve the physical layer security of OFDM-PON. From the characteristics of the scheme and the experiment results, we can see the novelty and impacts of this paper as follows:

(1) Compared with the direct encryption by using chaotic sequences, the DNA-RCS increases the randomness of chaotic sequences and provides higher security. It solves the problem of low security of low-dimensional chaos and complex realization of high-dimensional chaos. Since the implementation rules of the DNA-RCS are randomly selected, the illegal ONU cannot recover the correct data information. Besides, the DNA-RCS expands the application of the DNA code beyond the encryption of bit sequences.

(2) The proposed two-layer encryption makes permutation objects no longer limited to symbols or bit sequences alone. Compared with the traditional scrambling methods, it realizes non-repetitive permutation from symbols to units and ensures the high-security and high-efficiency encryption of the system. Also, combined with the plaintext-related diffusion, the encryption not only depends on the chaotic sequences but also relates to the order of permutation. The ciphertext enhances the ability to resist attackers.

(3) We first evaluate the provable security of the encryption scheme from the perspective of cryptanalysis. The key space provided by the scheme can reach 1.075×10^{91}. As the number of chaotic sequence blocks increases, the number of tests for an illegal ONU to break a secure transmission has increased exponentially, which can reach a maximum of 3.096×10^{106}. It can effectively resist various attacks without affecting the performance of the transmission system and improve the security of OFDM-PON.

REFERENCES

[1] B. Farhang-Boroujeny and H. Moradi, "OFDM inspired waveforms for 5G," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2474–2492, 4th Quart., 2016.

[2] C. DeSanti, L. Du, J. Guarin, J. Bone, and C. F. Lam, "Super-PON: An evolution for access networks [Invited]," *J. Opt. Commun. Netw.*, vol. 12, no. 10, p. D66, Oct. 2020.

[3] X. Fu, M. Bi, X. Zhou, G. Yang, Q. Li, Z. Zhou, and X. Yang, "A chaotic modified-DFT encryption scheme for physical layer security and PAPR reduction in OFDM-PON," *Opt. Fiber Technol.*, vol. 42, pp. 126–131, May 2018.

[4] X. Yang, Z. Shen, X. Hu, and W. Hu, "Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2499–2502, Nov. 15, 2016.

[5] M. Bi, X. Zhuo, X. Fu, X. Yang, and W. Hu, "Cellular neural network encryption scheme for time synchronization and CPAs resistance in OFDM-PON," *IEEE Access*, vol. 7, pp. 57129–57137, 2019.

[6] 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. 1, 2014.

[7] S. S. Li, M. F. Cheng, L. Deng, S. N. Fu, M. M. Zhang, M. Tang, P. Shum, and D. M. Liu, "Maximizing the security of digital chaos based OFDM-PON with a dynamical nonlinear transformation," presented at the 17th ICOCN, Zhuhai, China, 2019.

[8] Q. Chen, M. Bi, X. Fu, Y. Lu, R. Zeng, G. Yang, X. Yang, and S. Xiao, "Security scheme in IMDD-OFDM-PON system with the chaotic pilot interval and scrambling," *Opt. Commun.*, vol. 407, pp. 285–289, Jan. 2018.

[9] L. J. Zhang, B. Liu, and X. J. 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. 15, 2015.

[10] M. Bi, X. Fu, X. Zhou, L. Zhang, G. Yang, X. Yang, S. Xiao, and W. Hu, "A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON," *IEEE Photon. J.*, vol. 9, no. 1, pp. 1–10, Feb. 2017.

[11] J. Zhao, B. Liu, Y. Mao, J. Ren, X. Xu, X. Wu, L. Jiang, S. Han, and J. Zhang, "High-security physical layer in CAP-PON system based on floating probability disturbance," *IEEE Photon. Technol. Lett.*, vol. 32, no. 7, pp. 367–370, Apr. 1, 2020.

[12] W. Zhang, C. Zhang, C. Chen, W. Jin, and K. Qiu, "Joint PAPR reduction and physical layer security enhancement in OFDMA-PON," *IEEE Photon. Technol. Lett.*, vol. 28, no. 9, pp. 998–1001, May 1, 2016.

[13] 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. 15, 2017.

[14] T. W. Wu, C. F. Zhang, H. H. Wei, and K. Qiu, "PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM," *Opt. Exp.*, vol. 27, no. 20, pp. 27946–27961, Sep. 30, 2019.

[15] A. A. E. Hajomer, X. Yang, and W. Hu, "Secure OFDM transmission precoded by chaotic discrete Hartley transform," *IEEE Photon. J.*, vol. 10, no. 2, pp. 1–9, Apr. 2018.

[16] 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. Lightw. Technol.*, vol. 36, no. 9, pp. 1706–1712, May 1, 2018.

[17] T. Wu, C. Zhang, H. Huang, Z. Zhang, H. Wei, H. Wen, and K. Qiu, "Security improvement for OFDM-PON via DNA extension code and chaotic systems," *IEEE Access*, vol. 8, pp. 75119–75126, 2020.

[18] L. J. Zhang, B. Liu, X. J. Xin, and Y. J. Wang, "Joint robustness security in optical OFDM access system with Turbo-coded subcarrier rotation," *Opt. Exp.*, vol. 23, no. 1, pp. 13–18, Jan. 12, 2015.

[19] 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, pp. 1–10, Apr. 2017.

[20] A. Sultan, X. Yang, A. A. E. Hajomer, S. B. Hussain, and W. Hu, "Dynamic QAM mapping for physical-layer security using digital chaos," *IEEE Access*, vol. 6, pp. 47199–47205, 2018.

[21] Z. Hu and C.-K. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure Fast-OFDM-PON," *J. Lightw. Technol.*, vol. 36, no. 16, pp. 3373–3381, Aug. 15, 2018.

[22] X. M. Song, B. Liu, H. X. Zhang, R. Ullah, Y. Y. Mao, J. X. Ren, S. D. Chen, J. Y. Zhang, J. Y. Zhao, S. Han, X. Y. Liu, D. L. Zhao, and X. J. Xin, "Security-enhanced OFDM-PON with two-level coordinated encryption strategy at the bit-level and symbol-level," *Opt. Exp.*, vol. 28, no. 23, pp. 35061–35073, Nov. 9, 2020.

[23] Y. Xiao, Z. Wang, J. Cao, C. Long, Y. Chen, R. Deng, J. Shi, Y. Liu, and J. He, "Two-level encryption for physical-layer security in OFDM-PON based on multi-scrolls system," *Opt. Commun.*, vol. 440, pp. 126–131, Jun. 2019.

[24] H. Wei, C. Zhang, T. Wu, H. Huang, and K. Qiu, "Chaotic multilevel separated encryption for security enhancement of OFDM-PON," *IEEE Access*, vol. 7, pp. 124452–124460, 2019.

[25] A. Sultan, X. Yang, A. A. E. Hajomer, S. B. Hussain, and W. Hu, "Chaotic distribution of QAM symbols for secure OFDM signal transmission," *Opt. Fiber Technol.*, vol. 47, pp. 61–65, Jan. 2019.

[26] Y. Xiao, Z. Wang, J. Cao, R. Deng, Y. Liu, J. He, and L. Chen, "Time-frequency domain encryption with SLM scheme for physical-layer security in an OFDM-PON system," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 1, pp. 46–51, Jan. 2018.

[27] Z. Wang, F. Chen, W. Qiu, S. Chen, and D. Ren, "A two layer chaotic encryption scheme of secure image transmission for DCT pre-coded OFDM-VLC transmission," *Opt. Commun.*, vol. 410, pp. 94–101, Mar. 2018.

[28] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 235–246, Feb. 2016.

[29] L. Y. Zhang, Y. Liu, F. Pareschi, Y. Zhang, K.-W. Wong, R. Rovatti, and G. Setti, "On the security of a class of diffusion mechanisms for image encryption," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1163–1175, Apr. 2018.

[30] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.

[31] H. Wen and S. Yu, "Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 134, no. 7, p. 337, Jul. 2019.

[32] 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. 15, 2017.

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

[34] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018.

[35] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.

[36] G. Chen and T. Ueta, "Yet another chaotic attractor," *Int. J. Bifurcation Chaos*, vol. 9, no. 7, pp. 1465–1466, Jul. 1999.

MENGWEI CUI received the B.S. degree from Southwest Jiaotong University, Chengdu, China, in 2019. She is currently pursuing the M.S. degree with the University of Electronic Science and Technology of China, Chengdu. Her research interest includes secure access technology.

CHONGFU ZHANG (Senior Member, IEEE) received the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2009. From 2013 to 2014, he was a Visiting Scholar with the Optical Communications Laboratory (OCLAB), University of Southern California. He is currently a Full Professor with UESTC. He has authored or coauthored more than 100 articles and holds 70 patents. His research interests include broadband access networks, microwave photonics, communication security, and optical signal processing. He is a member of OSA. Along with his colleagues, he has received six awards in science and technology.

YUHANG CHEN received the B.S. degree from Dalian Maritime University, Dalian, China, in 2019. He is currently pursuing the M.S. degree with the University of Electronic Science and Technology of China, Chengdu, China. His research interests include broadband access networks and secure access technology.

ZHI ZHANG received the B.S. degree from Northeastern University, Shenyang, China, in 2018. He is currently pursuing the M.S. degree with the University of Electronic Science and Technology of China, Chengdu, China. His research interest includes secure access technology.

TINGWEI WU received the B.S. and M.S. degrees from Guizhou University, Guizhou, China, in 2014 and 2017, respectively. He is currently pursuing the Ph.D. degree with the University of Electronic Science and Technology of China, Chengdu, China. His research interests include cryptography, physical layer security, and OFDM security technology.

HEPING WEN received the M.S. and Ph.D. degrees from the Guangdong University of Technology, Guangzhou, China, in 2009 and 2019, respectively. He is currently a Lecturer with the Zhongshan Institute, University of Electronic Science and Technology of China. His research interests include chaos-based secure communication and image encryption.