IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 5, 2020, accepted April 17, 2020, date of publication April 21, 2020, date of current version May 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989172

Security Improvement for OFDM-PON via DNA Extension Code and Chaotic Systems

TINGWEI WU[1], CHONGFU ZHANG[1,2], (Senior Member, IEEE), HUAN HUANG[1], ZHI ZHANG[1], HANHAN WEI[1], HEPING WEN[1,2], AND KUN QIU[1]

[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 Project for National Key Research and Development Program of China under Grant 2018YFB1801302, in part by the National Science Foundation of China under 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, in part by the Zhongshan Innovative Research Team Program under Grant 180809162197886, in part by the Research Project for Talent of UESTC Zhongshan Institute under Grant 418YKQN07, and in part by the Sichuan Funded Project For Science and Technology under Grant 2018JY0145 and Grant CSC: 201906070008.

ABSTRACT In the paper, a deoxyribonucleic acid (DNA) extension code with 3-bit binary streams is proposed to encrypt the downlink data for orthogonal frequency division multiplexing passive optical network (OFDM-PON). It has 8 bases to make up 4 pairs of complementary codes. And it can obtain 384 matching rules, which greatly improves the randomness of matching. Here, two DNA addition operation rules are also proposed to encrypt the data. DNA extension rules can reduce half coding operations. Three 1-dimensional (1-D) chaotic systems are used to encrypt the code and control the rules. The encryption method based on the uplink streams from optical network units (ONUs) makes the security of downlink signals not just depending on the security of chaotic systems. Finally, a 22.06 Gb/s DNA extension code encryption signal is transmitted through a back-to-back (BTB) system and a 25-km standard single-mode fiber (SSMF). The proposed method not only improves the security but also reduces the computational complexity. The experimental results show that the proposed method has the ability to resist optical channel response and fiber nonlinearity, which is a promising candidate for solving the security enhancement in access networks.

INDEX TERMS DNA extension code, OFDM-PON, uplink stream, 1-D chaotic system, security enhancement.

I. INTRODUCTION

With the development of information technology, the 5th generation communication technology (5G) has begun to enter our lives. The main vision of 5G is the Internet of things (IoT) and a massive expansion of bandwidth. Orthogonal frequency division multiplexing (OFDM) is widely used in 5G communications. OFDM passive optical network (OFDM-PON) has the advantages including the resistance to chromatic dispersion, high spectral efficiency and anti-multipath interference [1]–[3], and it has been regarded as a promising candidate for the next generation communication. At the same time, people pay more attention to the information security. The conventional encryption and authentication operations are carried out in the upper layer. But the header information can be easily eavesdropped by the statistical attacks [4]. On the contrary, encryption in the physical layer can essentially protect the security of data transmission, then it has become a research hotspot. In 1963, Lorenz proposed the butterfly effect [5]. In the early 1980s, Lang and Kobayashi had been extensively examined the feedback semiconductor lasers [6]. From then on, chaos becomes a hot topic, such as dynamical behaviors of autonomous memristor chaotic systems [7] and time delay in memristor based neural network circuits [8]. Chaos has been applied to the computer science and communications. After that, various studies focus on the security of physical layer based on the chaotic techniques. These methods can be divided into two categories. One is the chaotic feedback laser such as secure key distribution [9], laser exclusive or (XOR) operation [10] and delay

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

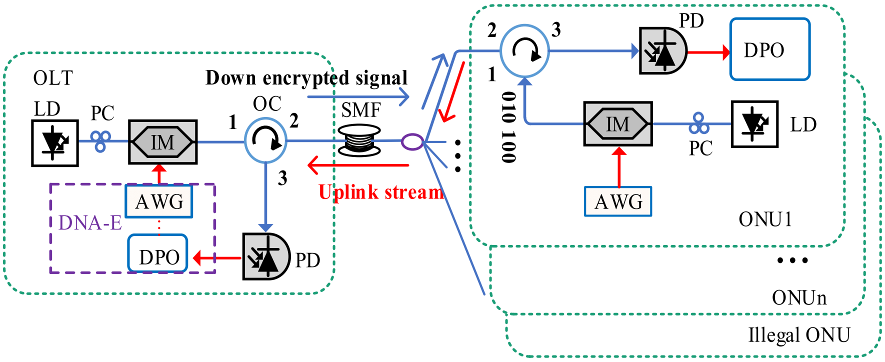


FIGURE 1. The configuration of proposed encryption method. (AWG: arbitrary waveform generator; LD: laser diode; IM: intensity modulator; SMF: single-mode fiber; TOA: tunable optical attenuator; PD: photodetector; OLT: optical line terminal; ONU: optical network unit; PC: polarization controller; OC: optical circulator; DPO: digital phosphor oscilloscope.)

signature-suppressed in semiconductor lasers [11], and the typical application in chaotic feedback laser and microwave photonic chaotic communication [12], [13]. These methods require two sets of chaos generation equipment to be as identical as possible, which are difficult to achieve chaos synchronization for all the modulation parameters. Meanwhile, Chen et. al deeply studied the chaotic system [14] and some digital chaotic image encryption methods have been proposed by many researchers [15]. The digital chaotic technique is the other way to encrypt the data transmission, because the digital chaos can be accurately controlled and easily operated by digital signal processing (DSP). Then it has been widely studied in OFDM-PON. In chaotic OFDM-PON communications, early typical studies are randomly transforming phase of constellation symbol [16] and 3-D constellation masking [17]. After that, various papers have emerged, such as constellation scrambling and permutation [18]–[20], phase masking and time-frequency confusion [21]–[23], short reference non-coherent system [24], pilot-aided secure key agreement [25], chaotic matrix transformation [26], [27], Brownian motion and chaos [28], [29], digital filter multiple access (DFMA)-PON [30], I/Q-encryption and constellation confusion [31], [32], joint peak to average power ratio (PAPR) reduction and encryption [33]–[35], differential chaos shift key [36], [37], multilevel separated encryption [38]. These methods have a common characteristic that the encryption algorithm depends on the pseudo-random numbers generated by the chaotic systems. When the chaotic system is cracked, the data is unsafe.

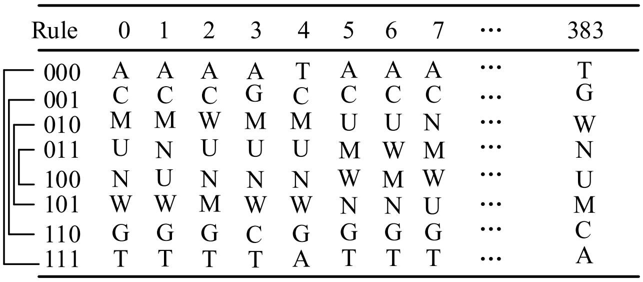
Meanwhile, Cao *et al.* proposed a method to encrypt the downlink stream by the uplink stream from an optical network unit (ONU) [39]. It encrypts the data by performing a simple XOR operation between the uplink stream and downlink stream. But the data encrypted by this method is vulnerable to illegal ONU attacks. Based on this case, Li *et al.* reported an improved scheme using the digital chaos algorithm and uplink stream with fixed-point implementation [40]. Compared with [39], it disturbs the chaotic bifurcation graph, which greatly raises the security for OFDM-PON.

Deoxyribonucleic acid (DNA) code has these advantages of huge storage, massive parallelism and ultra-low power consumption [41]. Chaotic DNA code can enhance the security of information science, so that it has been widely used in the image encryption [42], and its applications are also reported in OFDM-PON [43]. However, the extension of DNA code has not been studied yet.

In order to propose a high security and low computational complexity encryption algorithm for OFDM-PON, we propose a novel chaotic DNA extension code encryption algorithm. The conventional DNA code depends on 2-bit binary streams. Thus, our method uses 3-bit binary streams, which raises the randomness of coding. Besides, we also propose two addition operation rules corresponding to the DNA extension code. This encryption method uses the uplink streams from ONUs to improve the security of downlink streams. New coding rules can reduce half coding operations. Three 1-dimensional (1-D) chaotic systems are used to encrypt the code and control the rules. The proposed method not only improves the security but also reduces the computational complexity.

II. PRINCIPLES

We design a framework to transmit the uplink and downlink streams as shown in Fig. 1. If an ONU sends a series of bit streams, OLT receives the uplink streams and uses them to conduct the encryption process. In the field of biology, DNA has 4 kinds of bases, namely adenine (A), thymine (T), cytosine (C) and guanine (G), in which A-T and C-G are complementary pairs [44]. In the field of computer and information science, there are “1” and “0”, which are also complementary. In addition, for computer science, A, T, C, and G only stand for the bit-sequence symbols rather than the biomolecules. Thus, 2 bits can be used to represent 4 bases, and A-T and C-G in the DNA coding are replaced by 00-11 and 01-10. On this basis, we propose a DNA extension code, which uses 3 bits and another 4 bases M, W, U and N to express them. Assuming that M-W and U-N are complementary pairs, similar to 2-bit DNA code, we set 000-111,



Rule	0	1	2	3	4	5	6	7	⋯	383
000	A	A	A	A	T	A	A	A	⋯	T
001	C	C	C	G	C	C	C	C	⋯	G
010	M	M	W	M	M	U	U	N	⋯	W
011	U	N	U	U	U	M	W	M	⋯	N
100	N	U	N	N	N	W	M	W	⋯	U
101	W	W	M	W	W	N	N	U	⋯	M
110	G	G	G	C	G	G	G	G	⋯	C
111	T	T	T	T	A	T	T	T	⋯	A

FIGURE 2. The specific chaotic control of DNA extension rules.

001-110, 010-101 and 011-100 as complementary pairs namely A-T, C-G, M-W and

U-N. The matching rules are displayed as Fig. 2. One chaotic sequence is used to control the DNA extension matching rules.

For simplicity and convenience, we list some possible permutations of 3-bit DNA extension code as shown in the Fig. 2. Here, it is easy to figure out that the proposed 3-bit DNA extension code has $C_8^1 \times C_6^1 \times C_4^1 \times C_2^1 = 384$ matching rules, which is far more than that of 2-bit DNA coding ($C_4^1 \times C_2^1 = 8$). Obviously, the proposed method greatly raises the randomness of matching. If the uplink and downlink streams are identified by the chaotic DNA extension rules, the DNA addition operation will be conducted between two DNA extension codes. Hence, we design two DNA extension addition operation rules as listed in TABLE 1 and TABLE 2.

TABLE 1. Addition operation for DNA extension code (one).

+	A	C	M	U	N	W	G	T
A	N	W	G	T	A	C	M	U
C	W	N	T	G	C	A	U	M
M	G	T	N	W	M	U	A	C
U	T	G	W	N	U	M	C	A
N	A	C	M	U	N	W	G	T
W	C	A	U	M	W	N	T	G
G	M	U	A	C	G	T	N	W
T	U	M	C	A	T	G	W	N

The addition rules are symmetrical in structure and complementary to each other, which satisfies the Watson-Crick complementary regulation. We use another chaotic sequence to control the selection of addition rules for DNA extension code. Then the downlink signal is encrypted by the new chaotic DNA extension code with the uplink stream. The specific processes of encryption and decryption are based on chaotic DNA extension code, which can be illustrated in Fig. 3.

When receiving the uplink streams from ONUs, OLT begins to perform the encryption process. The operations are described step by step as follows:

TABLE 2. Addition operation for DNA extension code (two).

+	A	C	M	U	N	W	G	T
A	U	M	C	A	T	G	W	N
C	M	U	A	C	G	T	N	W
M	C	A	U	M	W	N	T	G
U	A	C	M	U	N	W	G	T
N	T	G	W	N	U	M	C	A
W	G	T	N	W	M	U	A	C
G	W	N	T	G	C	A	U	M
T	N	W	G	T	A	C	M	U

Step 1: Use the DNA extension rules to code the downlink and uplink streams as shown in the Fig. 2. Two chaotic sequences $\{x_1, x_2\}$ are utilized to handle the downlink and uplink streams respectively. The processing of chaotic sequences is

$$\begin{aligned}\{x_1\} &= \mathrm{mod}(\mathit{floor}(\dot{x}_1 \times 10^{14}), 384)\\ \{x_2\} &= \mathrm{mod}(\mathit{floor}(\dot{x}_2 \times 10^{14}), 384),\end{aligned} \tag{1}$$

where mod (α, β) and floor (φ) stand for the remainder operation and lower bound operation respectively. The processing of Eq. (1) can improve the randomness of chaotic sequences.

Step 2: The chaotic sequence $\{x_3\}$ is applied to choose the addition operation rules as displayed in TABLE 1 and TABLE 2. $\{x_3\}$ can be generated by

$$\{x_3\} = \mathrm{mod}(\mathit{floor}(\dot{x}_3 \times 10^{14}), 2). \tag{2}$$

Step 3: After **Step 2,** the downlink signal is encrypted by the uplink stream and chaotic DNA extension code. In this case, the encrypted signal is a DNA extension code, which cannot be directly transmitted. Therefore, a fixed conversion standard [A C M U N W G T] → [000 001 010 011 100 101 110 111] is used to convert a DNA extension code into bit streams. Of course, another chaotic sequence can also be used to encrypt this step.

From now on, various chaotic systems are proposed by scholars. For convenience, we need 3 chaotic sequences to encrypt the code. Therefore, the logistic sine system (LSS), logistic tent system (LTS) and tent sine system (TSS) [45] are chosen to generate the pseudo-random numbers respectively.

$$\begin{aligned}w_{n+1} &= LSS(r, w)\\ &= (rw_n(1-w_n) + (4-r)\sin(\pi w)/4) \bmod 1,\end{aligned} \tag{3}$$

$$\begin{aligned}y_{n+1} &= LTS(r, y_n)\\ &= \begin{cases}(ry_n(1-y_n) + (4-r)y_n/2) \bmod 1 & v_n < 0.5\\ (ry_n(1-y_n) & \\ +(4-r)(1-y_n)/2) \bmod 1 & v_n \geq 0.5,\end{cases}\end{aligned} \tag{4}$$

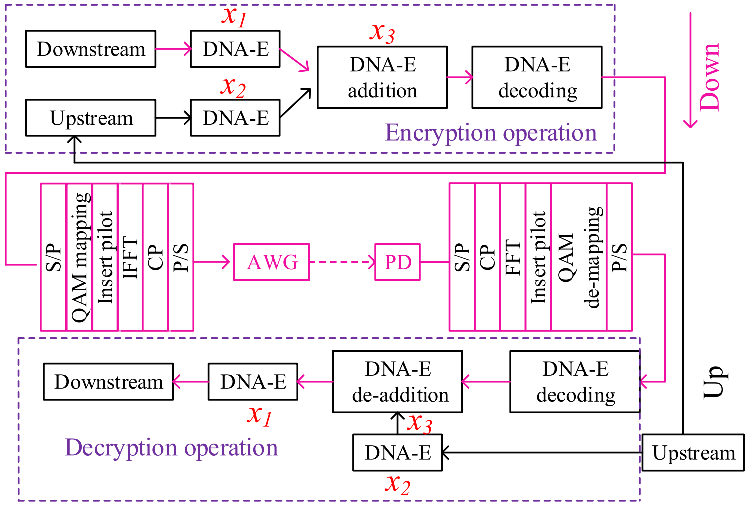


FIGURE 3. The integral flow chart for encryption and decryption.

$$
\begin{aligned}
z_{n+1} &= TSS(r, z_n)\\
&= \begin{cases} (rz_n/2 + (4-r)\sin(\pi z_n)/4) \bmod 1 & \delta_n < 0.5\\ (r(1-z_n)/2 & \\ +(4-r)\sin(\pi z_n)/4) \bmod 1 & \delta_n \geq 0.5, \end{cases}
\end{aligned}
\tag{5}
$$

where r is the bifurcation coefficient. When $r \in (0\ 4)$ and the initial values of w, y, z $\in (0, 1)$, the LSS, TLS and TSS chaotic systems have good chaotic behaviors.

For the decryption, the detailed processes are displayed in the below of Fig. 3. When the transmission signal is detected by a photodetector (PD), the ONU can obtain the encrypted signal after conducting the operations such as removing CP and QAM de-mapping. The detailed operations are as follows:

Step 1: Convert the encrypted bit streams into a DNA extension code by the fixed conversion standard [A C M U N W G T] → [000 001 010 011 100 101 110 111].

Step 2: This method adopts the symmetric encryption technology. An ONU combines the pre-shared key with Eqs. (1)-(3) to generate chaotic sequences $\{x_2\}$ to encrypt the uplink stream sent by itself.

Step 3: Based on **Step 2**, $\{x_3\}$ can also be obtained to choose the same DNA extension addition rules as the ***Step 2 in encryption process***. After that, we get the encrypted DNA extension code.

Step 4: Chaotic sequences $\{x_1\}$ are used to decrypt the encrypted DNA extension code and obtain the downlink stream based on Fig. 2.

III. RESULTS AND DISCUSSIONS

To test the performance of the chaotic systems, we first simulate the initial sensitivity performances of LSS, TSS, and TLS. The initial values of r is set to 0.5 and w, y, z are set to 0.7. When the initial values of w, y, z have a tiny difference of $\Delta = 10^{-15}$, the chaotic sequences can be shown in the Fig. 4. From the results, it is easy to conclude that every two chaotic sequences are completely different after dozens of iterations. The detailed performance of LSS, TSS, and TLS are listed in the Fig. 4(a), Fig. 4(b) and Fig. 4(c).

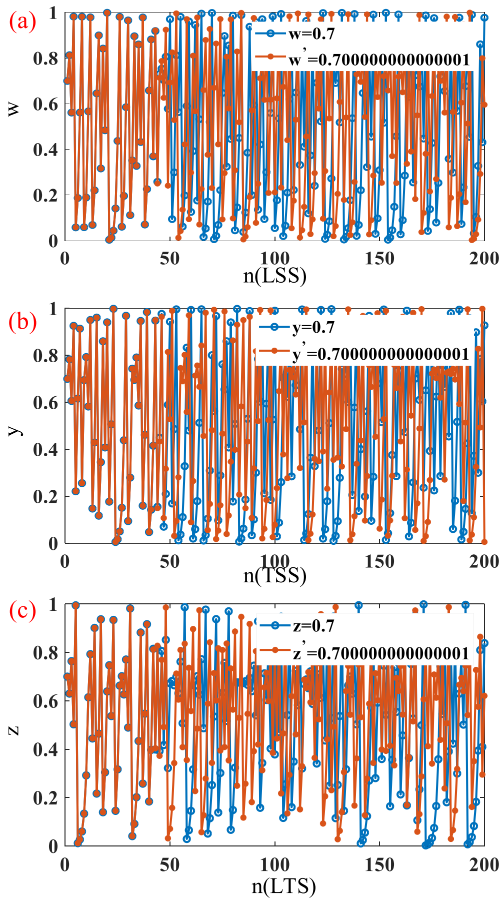


FIGURE 4. The sensitivity of (a) LSS, (b) TSS and (c) LTS with initial value differences of 10^{-15}.

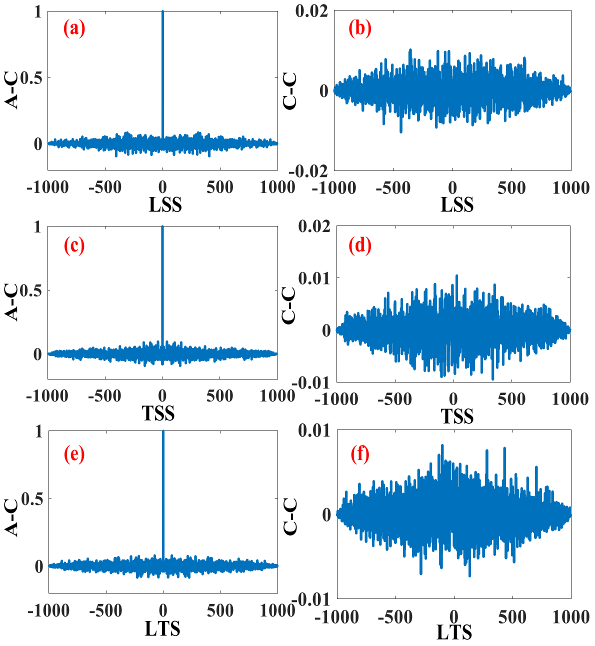


FIGURE 5. (a) The auto-correlation (A-C) of LSS, (b) the cross-correlation (C-C) of LSS, (c) the A-C of TSS, (d) the C-C of TSS, (e) the A-C of LTS and (f) the C-C of LTS.

Additionally, we have tested the auto-correlation and cross-correlation performance of the used 3 chaotic systems. When r is also set to 0.5 and w, y, z are set to 0.7, we iterate 1000 chaotic sequences and the results can be seen as Fig. 5. From Fig. 5(a), Fig. 5(c) and Fig. 5(e), only when the values are equal to 0, auto-correlation values are equal to 1, and other values are close to 0, which indicates that they have good auto-correlation performance. When we also give a tiny difference of $\Delta = 10^{-15}$ (the related sequences are in the Fig. 4), the cross-correlation performance of the chaotic system can be shown as Fig. 5(b), Fig. 5(d) and Fig. 5(f). Variation of all values is in $[-0.01, 0.01]$, which indicates that they have good performance in cross-correlation.

TABLE 3. The comparisons of different related chaotic systems.

	Chaotic systems in the paper	7-D chaos (Ref. [49])	4-D chaos (Ref. [48])	Chen's attractor [47]	Logistic Map (Ref. [46])
Addition	9	234	41	41	1
Multiplication	15	215	54	38	2
Sine function	3	4	8	0	0
Key space	6.4×10^{91}	$>10^{105}$	$10^{70.7}$	10^{45}	$10^{21.4}$

In order to further study the performance of the used chaotic system, some comparisons between it and other chaotic systems are shown in TABLE 3. One can find that our used chaotic systems have low computational complexity and high security. In fact, LSS, TSS and TLS are evolved from the Logistic map [46] and the three chaotic systems have a more secure performance than the logistic map. Of course, their computational complexities are tiny higher than logistic map. Compared with other chaotic systems, the used chaotic systems have low computational complexity, but its security is not low. Because the key space is bigger than Chen's attractor [47] and 4-D chaos [48]. These hyper-chaotic systems use the fourth-order Runge-Kutta method, which have the time complexity of O(N^3) as the order increasing. Therefore, 7-D IQ [49] has the highest computational complexity.

TABLE 4. The comparisons of different related chaotic systems.

	DNA-E code	DNA code
Bit number	3	2
Code number	8	4
Pair	4	2
Matching rule	384	8
Addition operation	64	16

The performance comparisons between the chaotic DNA extension code and conventional chaotic DNA code are listed in TABLE 4. The conventional DNA code uses 2 bits per unit, but the DNA extension code uses 3 bits. If the data is a fixed bit stream, using the DNA extension code can halve the operations. The conventional DNA code has 4 bases (A, T, C and G) and the DNA extension code adds another 4 bases (M, W, U, and N). From this case, DNA code and DNA extension code have 2 and 4 complementary pairs respectively. The conventional DNA code has 8 matching rules, while the DNA extension code has 384 matching rules. In addition, there are $8^2 = 64$ kinds of addition/subtraction operations for the DNA extension code. More importantly, since this encoding method is a set of 3 bits, compared with the traditional method (2 bits), it will reduce the amount of calculation by half. Additionally, combined with [39], the DNA extension addition operations between the uplink data and downlink data have higher security than operations on itself.

In the experiment, we randomly generate two sets of bit flow with a length of 1.92×10^5. One of them is regarded as the uplink stream, and the other is considered as the downlink stream, which is then encrypted via the uplink stream and DNA extension code. These processes are conducted offline by MATLAB. After that, the bit streams are transformed into 4.8×10^4 16-QAM symbols. Serial-to-parallel (S/P) conversion is used in OFDM modulation and the number of subcarriers is 120. IFFT converts these symbols from the frequency domain into the time domain and its size is 256. A cyclic prefix (CP) of 1/16 is inserted in each sequence. When the encryption process is over, the encrypted signal is loaded into an arbitrary waveform generator (AWG Tektronix 7102A) to complete the digital-to-analog conversion (DAC) with a sampling rate of 25 GSa/s. The electrical signal is then modulated to a Mach-Zehnder modulator (MZM). A tunable laser diode emits light with a wavelength of 1549nm and its output power is 14.48 dBm. Here, the initial values of w, y,

TABLE 5. The comparisons of different related chaotic encryption methods.

	DNA-E	HCCD [20]	CCT [25]	BSS [29]	DNA [43]	7-D IQ [49]
Addition	3N	2N	12N	18N	4.5N	58.5N
Multiplication	6N	6N	13N	26N	3N	53.75N
other	5N	(N×log$_2$N)/2+3N	5N	10N	6N	8N
T	*O*(N)	*O*(N×log$_2$N)	*O*(N)	*O*(N)	*O*(N)	*O*(N)
Key space	6.4×10^{91}	10^{60}	4×10^{30}	2.7×10^{90}	2.25×10^{89}	$>10^{105}$

Note: T stands for the time complexity.

z, r are set as 0.7 0.7 0.7, 0.5 respectively, which are saved as the key. The generated key space is $(4 \times 10^{15} \times 10^{15})^3 = 6.4 \times 10^{91}$, which is strong enough to resist exhaustive attacks from an illegal ONU.

Assuming that transmission the same length of bit sequences and comparing with some typical chaotic OFDM-PON encryption systems such as the hybrid chaotic confusion and diffusion (HCCD) [20], chaotic constellation transformation (CCT) scrambling [25], Brownian motion symbol substitution (BBS) [29], real and imaginary (IQ) parts encryption [31] and 7-D IQ encryption [49], some important parameters are listed in TABLE 5. Their comparisons mainly focus on the computational complexity of chaotic pseudo-random number generator (PRNG) and encryption. Our proposed DNA-E has almost the lowest computational complexity and the security performance is high. Compared with a conventional DNA encryption method, although our method uses a more complex and secure system, it is worth noting that its computational complexity is also lower than the traditional method. For example, [43] uses a simpler chaotic system, but its computational complexity of the system is greater and the key space is smaller. As a high-order hyper-chaotic system, the complexity of [49] is high. This means that the computational complexity of [49] is much greater than other common chaotic encryption systems. Therefore, it is should be careful when we choose a high-order hyper-chaotic system. Because we use the fourth-order Runge-Kutta method to calculate, the hyper-chaotic systems will rapidly increase the complexity of the systems.

PAPR is a significant parameter for an OFDM system. Hence, we calculate the complementary cumulative distribution functions (CCDFs) of PAPR for the encrypted and original signals. The results in Fig. 6 indicate that the PAPR performance of chaotic DNA extension code encryption signal is almost the same as the original signal. Thus, the proposed encryption method does not deteriorate the system performance.

When the encrypted downlink stream transmits over a back-to-back (BTB) system and a 25-km SSMF, it is detected by a photodetector (PD) with a bandwidth of 10 GHz. The data is recorded by a digital phosphor oscilloscope (DPO Tektronix TDS 7404B) with a sampling rate of 50 GSa/s. The decryption operations are also done offline by MATLAB with the pre-shared key and the corresponding uplink stream.

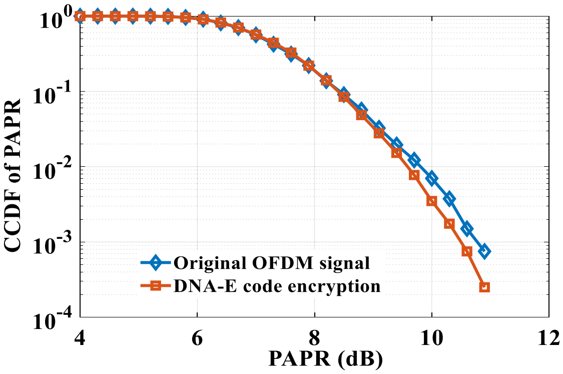


FIGURE 6. CCDF curves of DNA extension code encryption signal and original OFDM signal.

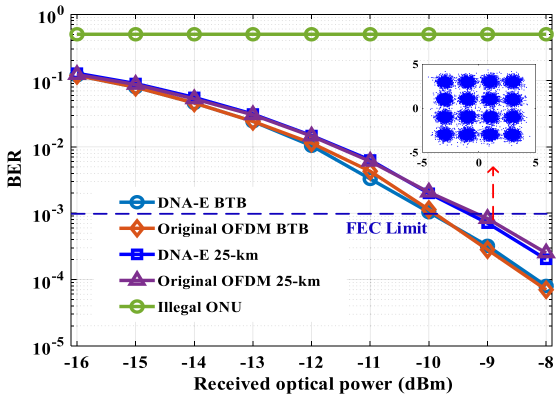


FIGURE 7. The BER performances of original and DNA extension code encryption signals.

Fig. 7 shows that the original OFDM signal and chaotic DNA extension code encryption signal have basically the same bit error rate (BER) performance in the BTB system. Owing to the fiber dispersion and loss, the BERs of the two signals transmitted through a 25-km SSMF are approximately 0.7 dBm received optical power (FEC limit) lower than that of BTB systems, which means that the proposed method has the ability to resist fiber nonlinearity.

IV. CONCLUSION

In this paper, a DNA extension code combing three 1-D chaotic systems to enhance the physical layer security for OFDM-PON has been proposed and experimentally demonstrated. It aims at improving the security and reducing the computational complexity. A 22.06 Ga/s encrypted OFDM signal has been transmitted through a BTB system and a 25-km SSMF. The following conclusions can be obtained:

1) The DNA extension code with 3-bit binary streams is evolved from the conventional DNA code. It meets the DNA coding rules in chaotic encryption for OFDM-PON, and it is also suitable for computer science and image encryption. Compared with the conventional DNA code, the DNA extension code needs another 4 bases to express 8 complementary codes. It is worth noting that the DNA extension code can generate 384 kinds of matching rules, which highly raises the randomness and unpredictability of matching. In addition, the proposed two DNA addition operation rules can decrypt the signals correctly. Furthermore, the DNA extension code can also be extended to 4-bits or more, which is similar to the 4-QAM, 8-QAM, 16-QAM etc. However, the extension requires a redesign of some rules like the addition operation rules. Compared with conventional DNA chaotic coding encryption techniques, it is worth noting that the DNA extension code can reduce the half computational complexity.
2) Adopting the method that using the uplink stream to encrypt the downlink stream can make the transmission security not completely dependent on the chaotic systems, which provides better security than the conventional encryption method. If a secure hash algorithm is applied to generate the secured keys from the uplink stream, the security can be further enhanced.

It can be seen from the above conclusions that the proposed method is a promising candidate for the next generation security access network.

REFERENCES

[1] F. Carvalho and A. Cartaxo, "Multisignal OFDM-based hybrid optical-wireless WDM LR-PON with colorless ONU," *IEEE Photon. Technol. Lett.*, vol. 27, no. 11, pp. 1193–1196, Jun. 1, 2015.

[2] C. Zhang, Q. Zhang, C. Chen, N. Jiang, D. Liu, K. Qiu, S. Liu, and B. Wu, "Metro-access integrated network based on optical OFDMA with dynamic sub-carrier allocation and power distribution," *Opt. Express*, vol. 21, no. 2, pp. 2474–2479, Jan. 2013.

[3] S.-Y. Jung, C.-H. Kim, S.-M. Jung, and S.-K. Han, "Optical pulse division multiplexing-based OBI reduction for single wavelength uplink multiple access in IM/DD OFDMA-PON," *Opt. Express*, vol. 24, no. 25, pp. 29198–29208, Dec. 2016.

[4] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[5] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, Jan. 1963.

[6] R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," *IEEE J. Quantum Electron.*, vol. 16, no. 3, pp. 347–355, Mar. 1980.

[7] J. Sun, X. Zhao, J. Fang, and Y. Wang, "Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization," *Nonlinear Dyn.*, vol. 94, no. 4, pp. 2879–2887, Dec. 2018.

[8] J. Sun, G. Han, Z. Zeng, and Y. Wang, "Memristor-based neural network circuit of full-function pavlov associative memory with time delay and variable learning rate," *IEEE Trans. Cybern.*, early access, Nov. 21, 2019, doi: 10.1109/TCYB.2019.2951520.

[9] C. Xue, N. Jiang, Y. Lv, and K. Qiu, "Secure key distribution based on dynamic chaos synchronization of cascaded semiconductor laser systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 312–319, Jan. 2017.

[10] T. Kodama, N. Nakagawa, N. Kataoka, N. Wada, G. Cincotti, X. Wang, T. Miyazaki, and K.-I. Kitayama, "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, Jan. 1, 2010.

[11] A. Zhao, N. Jiang, S. Liu, C. Xue, and K. Qiu, "Wideband time delay signature-suppressed chaos generation using Self-Phase-Modulated feedback semiconductor laser cascaded with dispersive component," *J. Lightw. Technol.*, vol. 37, no. 19, pp. 5132–5139, Oct. 1, 2019.

[12] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Perquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fiber-optic links," *Nature*, vol. 438, pp. 343–346, Nov. 2005.

[13] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nature Photon.*, vol. 9, no. 3, pp. 151–162, Mar. 2015.

[14] Y. Li, W. K. S. Tang, and G. Chen, "Generating hyperchaos via state feedback control," *Int. J. Bifurcation Chaos*, vol. 15, no. 10, pp. 3367–3375, Oct. 2005.

[15] J. Chen, Z. L. Zhu, L. B. Zhang, Y. Zhang, and B. Q. Yang, "Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption," *Signal Process.*, vol. 142, pp. 340–353, Jul. 2017.

[16] B. Liu, L. Zhang, X. Xin, and J. Yu, "Constellation-masked secure communication technique for OFDM-PON," *Opt. Express*, vol. 20, no. 22, pp. 25161–25168, Oct. 2012.

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

[18] 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.

[19] 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. 15, 2014.

[20] 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.

[21] 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, Feb. 2017, Art. no. 7901510.

[22] M. Bi, T. Huang, L. Liu, X. Miao, S. Xiao, and W. Hu, "Performance optimization by nonparametric histogram estimation for low resolution in IMDD-OQAM-OFDM system," *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 7905013.

[23] X. Li, L. Deng, X. Chen, H. Song, Y. Liu, M. Cheng, S. Fu, M. Tang, M. Zhang, and D. Liu, "Arbitrary bias point control technique for optical IQ modulator based on dither-correlation detection," *J. Lightw. Technol.*, vol. 36, no. 18, pp. 3824–3836, Sep. 15, 2018.

[24] G. Kaddoum, E. Soujeri, and Y. Nijsure, "Design of a short reference non-coherent chaos-based communication systems," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 680–689, Feb. 2016.

[25] 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 1, 2017.

[26] 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.

[27] 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.

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

[29] W. Zhang, C. Zhang, C. Chen, H. Zhang, and K. Qiu, "Brownian motion encryption for physical-layer security improvement in CO-OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 12, pp. 1023–1026, Jun. 15, 2017.

[30] C. Zhang, Y. Yan, T. Wu, X. Zhang, G. Wen, and K. Qiu, "Phase masking and time-frequency chaotic encryption for DFMA-PON," *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 7203009.

[31] W. Zhang, C. F. Zhang, W. Jin, C. Chen, N. Jiang, and K. Qiu, "Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON," *IEEE Photon. Technol. Lett.*, vol. 26, no. 19, pp. 1964–1967, Oct. 1, 2014.

[32] 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.

[33] 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.

[34] 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.

[35] 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. 27946–27960, Sep. 2019.

[36] W. Xu, T. Huang, and L. Wang, "Code-shifted differential chaos shift keying with code index modulation for high data rate transmission," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4285–4294, Oct. 2017.

[37] W. Xu, Y. Tan, F. C. M. Lau, and G. Kolumban, "Design and optimization of differential chaos shift keying scheme with code index modulation," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 1970–1980, May 2018.

[38] 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.

[39] P. Cao, X. Hu, J. Wu, L. Zhang, X. Jiang, and Y. Su, "Physical layer encryption in OFDM-PON employing time-variable keys from ONUs," *IEEE Photon. J.*, vol. 6, no. 2, Apr. 2014, Art. no. 7901006.

[40] S. Li, M. Cheng, L. Deng, S. Fu, M. Zhang, M. Tang, P. Shum, and D. Liu, "Secure strategy for OFDM-PON using digital chaos algorithm with fixed-point implementation," *J. Lightw. Technol.*, vol. 36, no. 20, pp. 4826–4833, Oct. 15, 2018.

[41] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[42] Y. Wang, P. Lei, H. Yang, and H. Cao, "Security analysis on a color image encryption based on DNA encoding and chaos map," *Comput. Electr. Eng.*, vol. 46, pp. 433–446, Aug. 2015.

[43] 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.

[44] Q. Zhang, L. Guo, X. Xue, and X. Wei, "An image encryption algorithm based on DNA sequence addition operation," in *Proc. 4th Int. Conf. Bio-Inspired Comput.*, Oct. 2009, pp. 1–5.

[45] X. Chai, "An image encryption algorithm based on bit level brownian motion and new chaotic systems," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 1159–1175, Jan. 2017.

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

[47] G. Chen and T. Ueta, "Yet another chaotic attractor," *Int. J. Bifurcation Chaos*, vol. 09, no. 07, pp. 1465–1466, Jul. 1999.

[48] K. Sun, X. Liu, C. Zhu, and J. C. Sprott, "Hyperchaos and hyperchaos control of the sinusoidally forced simplified lorenz system," *Nonlinear Dyn.*, vol. 69, no. 3, pp. 1383–1391, Aug. 2012.

[49] Z. Hu and C. 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.

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.

CHONGFU ZHANG (Senior Member, IEEE) received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2009. From 2013 to 2014, he was a Visiting Scholar with the OCLAB, University of Southern California. He is currently a Full Professor with UESTC. He has authored or coauthored over 100 articles and holds 40 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 of science and technology.

HUAN HUANG received the B.S. degree from Anhui University, Anhui, China, in 2016, and the M.S degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2019, where he is currently pursuing the Ph.D. degree. His research interests include microwave photonics and optical wireless access networks.

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.

HANHAN WEI received the B.S. degree from the Beijing University of Technology, Beijing, China, in 2017. She is currently pursuing the M.S. degree with the University of Electronic Science and Technology of China, Chengdu, China. Her research interest includes secure access 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.

KUN QIU received the M.S. and Ph.D. degrees from Tsinghua University, Beijing, China, in 1987 and 1990, respectively. He is currently a Full Professor and a Ph.D. Supervisor of optical communications with UESTC. He has authored/coauthored over 200 scientific articles and the book of Optical Fiber Communication. His research interests include optical communications, broadband access networks, and optical signal processing. He was the Chair of the Chengdu Chapter, IEEE Photonics Society.