Enhanced Physical Layer Security and PAPR Performance Based on Disturbance of Data Cluster Under Chaotic Sequence Color Seeking Mechanism in CO-OFDM System

Le Liu, Xianfeng Tang, Fan Li, Zeyu Xu, and Xiaoguang Zhang

***Abstract*—This study proposes a physical layer encryption scheme based on disturbance of data cluster under color seeking mechanism of chaotic sequence which is generated by Brownian motion determined by keys aiming to improve security of coherent optical orthogonal frequency division multiplexing (CO-OFDM) system. Chaotic sequences with good randomness and unpredictability are endowed with a unique color composed of two primary colors and go through order transformation by sorting and seeking, which forms the chaotic sequence color seeking mechanism. The disturbance of transmitted data is realized according to chaotic sequence color seeking mechanism and PAPR performance is optimized simultaneously. The security of system is enhanced due to a key space of 10^{90} and PAPR can be reduced by 0.5 dB. An experiment conducted in a 40 GHz 16QAM CO-OFDM system over an 80 km standard single mode fiber (SSMF) shows that the authorized user can successfully decrypt the received signal, while the eavesdroppers cannot derive valid information with bit error rate (BER) at approximately 0.5. Analyses of peak to average power ratio (PAPR) performance and time complexity of the scheme are further carried out under different cluster forming methods to derive the optimized configuration which is critical in encryption.**

***Index Terms*—Brownian motion, chaotic sequence color seeking mechanism, CO-OFDM, PAPR, physical layer encryption.**

Manuscript received 11 March 2023; revised 31 May 2023 and 16 June 2023; accepted 17 June 2023. Date of publication 20 June 2023; date of current version 16 October 2023. This work was supported in part by the National Natural Science Foundation of China under Grants 62001040 and 62271517, in part by the Fund of State Key Laboratory of IPOC (BUPT) under Grant IPOC2021ZT12, in part by the Fundamental and Applied Basic Research Project of Guangzhou City under Grant 202002030326, in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2023B1515020003, in part by the Open Fund of IPOC (BUPT) under Grant IPOC2020A010, and in part by the BUPT Excellent Ph.D. Students Foundation under Grant CX2022120. *(Corresponding authors: Xianfeng Tang; Fan Li.)*

Le Liu, Xianfeng Tang, Zeyu Xu, and Xiaoguang Zhang are with the State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: leliu@bupt.edu.cn; tangxianfengbupt@bupt.edu.cn; xuzeyu2018@bupt.edu.cn; xgzhang@bupt.edu.cn).

Fan Li is with the School of Electronics and Information Technology, Guangdong Provincial Key Laboratory of Optoelectronic Information Processing Chips and Systems, Sun Yat-Sen University, Guangzhou 510275, China (e-mail: lifan39@mail.sysu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JLT.2023.3288035.

Digital Object Identifier 10.1109/JLT.2023.3288035

I. Introduction

COHERENT optical orthogonal frequency division multiplexing (CO-OFDM) technology has been extensively investigated and widely applied in optical fiber communication systems owing to its high spectral efficiency and flexible modulation format, which can effectively suppress the influence of dispersion and nonlinear effect of optical fiber link in optical communication systems [1], [2], [3]. However, the security of optical communication system is threatened by optical fiber eavesdropping technologies [4], [5], [6], [7]. Therefore, it is necessary to strengthen the security performance of CO-OFDM system.

Physical layer encryption for optical fiber communication system has extensive garnered attention in research on account of its transparency to upper protocols and complete protection for the transmitted data, while simultaneously it is able to directly combine with the digital signal processing (DSP) to reduce complexity [8], [9], [10]. Many encryption schemes have been proposed by researchers such as bit and symbol encryption [11], [12], [13], amplitude spreading [14], [15], frequency transformation [16], [17], [18], phase scrambling [19], [20], [21], [22] and encryption with state of polarization [23], [24], which can effectively enhance the security performance of system.

Recently, many studies propose to utilize chaotic system to achieve physical layer encryption, which can effectively enhance the randomness of encryption and security performance of system [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42]. However, as an important system performance metric of OFDM signal, peak to average power ratio (PAPR) is generally optimized independently with security enhancement process, which can lead to deterioration of decryption performance. Enhancing both security and PAPR performance simultaneously can be challenging without using additional operations to reduce PAPR. To overcome this, we propose an encryption scheme based on disturbance of OFDM data cluster by chaotic system in frequency domain, and simultaneously PAPR can be reduced through this frequency domain scrambling algorithm. Thus, enhancement of security and PAPR performance for CO-OFDM system is jointly realized in the

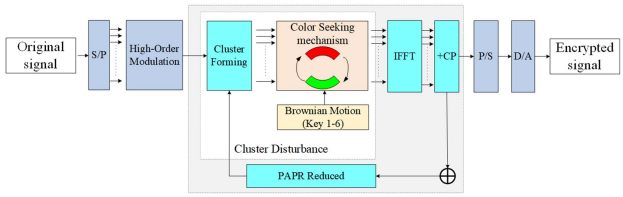

Fig. 1. Schematic diagram of the proposed encryption scheme at OFDM transmitter.

proposed scheme by optimizing frequency domain encryption operation.

In this study, we propose a physical layer encryption scheme based on disturbance of data cluster under chaotic sequence color seeking mechanism in CO-OFDM, wherein chaotic sequences are generated with a random and unpredictable Brownian motion (BM) decided by 6 keys. OFDM signal is divided via a specific cluster forming method into blocks with identical size. These blocks are endowed with different colors composed of two primary colors, red and green, ranging from 0 to 255 with equal difference increments. Meanwhile, two chaotic sequences generated by Brownian motion are sorted respectively in ascending order to get two ordered chaotic sequences. The new derived sequences are each represented by a primary color, and elements in the sequences are assigned intensities of corresponding primary color following the same rule with original OFDM data blocks. The position transformation rule of the same color between original and new sequences creates the chaotic sequence color seeking mechanism. Each data block with unique color looks for new coordinate positions according to the chaotic sequence color seeking mechanism, after which the disturbance of data cluster is achieved. With enhanced security performance, PAPR is simultaneously decreased through the scrambling of data cluster owing to the breakdown of the phase transition relationship between adjacent symbols.

An experiment was successfully conducted to verify the proposed physical layer security and PAPR performance enhanced transmission scheme in a CO-OFDM system with net data rate of 124 Gb/s over an 80 km standard single mode fiber (SSMF). The obtained results indicate that the proposed encryption scheme greatly enhances the system security performance with the key space of 10^{90} while PAPR is reduced by 0.5 dB.

II. Principle

Fig. 1 shows the schematic diagram of security and PAPR performance jointly enhanced physical layer encryption scheme based on disturbance of data cluster under chaotic sequence color seeking mechanism using Brownian motion with 6 keys at OFDM transmitter. Firstly, the original signal goes through cluster forming after series-parallel conversion and high-order modulation, which divides the signal into blocks of the same size and each block is given an unique color. Subsequently according to the chaotic sequence color seeking mechanism constructed by two chaotic sequences from Brownian motion, each block with a color seeks for a new location of the same color, which implements the disturbance of data cluster. Then the encrypted OFDM is obtained after transforming disturbed data cluster via inverse fast Fourier transform (IFFT) and appending cyclic prefix (CP). At this time, the PAPR of signal is calculated and fed back to adjust cluster forming method so that the matched method under optimal PAPR performance is selected, which realizes the enhancement of the PAPR performance. Finally, the encrypted signal is obtained through parallel-series and digital-to-analog conversion. Consequently, the encrypted CO-OFDM signal is transmitted through an optical fiber channel and coherently received at the receiving end. After compensating the channel distortion, the corresponding decryption steps are implemented to derive the information at the legal receiver by reversing the encryption process.

The chaotic sequence color seeking mechanism is a position scrambling algorithm based on the color transformation relationship using two chaotic sequences generated by Brownian motion. Brownian motion is a kind of random motion which exists in nature objectively and describes the random motion of particles suspended in fluid. By abstracting and simulating this random motion, a mathematical model with strong randomness can be obtained, where two chaotic sequences X and Y are generated to be used for encryption. The position coordinates (x, y) of a particle in two-dimensional plane form two chaotic sequences. Brownian motion can be expressed as

$$\begin{aligned} dx &= \tau \sin a \cos b \\ dy &= \tau \sin a \sin b \\ a &= u \times 2\pi, b = v \times 2\pi, \end{aligned} \tag{1}$$

where τ is the polar radius representing step size, parameters a and b are polar angles of u and v which decide the direction of motion. Therefore, the mathematical model of Brownian motion is determined by three parameters, τ, u and v, and these three parameters are respectively generated by three random systems, TSS (Tent-Sine System), LSS (Logistic-Sine System) and LTS (Logistic-Tent System), as shown in (2).

$$\begin{aligned} u_{n+1} &= LSS(p_u, u_n) \\ &= (p_u u_n(1-u_n) + (4-p_u)\sin(\pi u_n)/4) \bmod 1 \\ v_{n+1} &= LTS(p_v, v_n) = \\ &\begin{cases} (p_v v_n(1-v_n) + (4-p_v)v_n/2) \bmod 1, if v_n < 0.5 \\ (p_v v_n(1-v_n) + (4-p_v)(1-v_n)/2) \bmod 1, if v_n \geq 0.5 \end{cases} \\ \tau_{n+1} &= TSS(P_\tau, \tau_n) = \\ &\begin{cases} (p_\tau \tau_n/2 + (4-p_\tau)\sin(\pi\tau_n)/4) \bmod 1, if \tau_n < 0.5 \\ (p_\tau(1-\tau_n)/2 + (4-p_\tau)\sin(\pi\tau_n)/4) \bmod 1, if \tau_n \geq 0.5 \end{cases} \end{aligned} \tag{2}$$

p_u, p_v, p_τ are three system parameters affecting the output of Brownian motion. Initial values u_0, v_0, τ_0 and p_u, p_v, p_τ are selected as 6 keys owing to the sensitivity of the chaotic system to initial value, which further decides the chaotic sequences X and Y generated by Brownian motion.

Fig. 2 shows the principle of chaotic sequence color seeking mechanism. OFDM signal can be described as a matrix with rows representing subcarriers and columns representing symbols

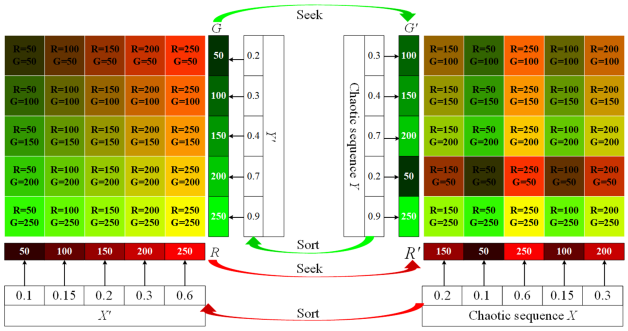

Fig. 2. Schematic diagram of the chaotic sequence color seeking mechanism.

on each carrier. As shown on the left in Fig. 2, the OFDM signal is divided into blocks of data with same size after cluster forming. Each block is endowed with an unique color composed of two primary colors with gradient red and green ranging from 0 to 255.

In order to realize the mapping from chaotic sequences to corresponding primary colors, the random chaotic sequences *X* and *Y* are first sorted to get the ordered sequences X' and Y':

$$X' = Sort(\text{chaotic sequence } X)$$
$$Y' = Sort(\text{chaotic sequence } Y) \tag{3}$$

The two ordered sequences are endowed with red(R) and green(G) colors of gradient intensities respectively through coloring operation *C* in (4).

$$R = C\left(X'\right) \quad G = C\left(Y'\right) \tag{4}$$

The gradient color sequences *R* and *G* are also used as horizontal and vertical coordinates of the original OFDM signal respectively. Color sequences R' and G' which correspond to the horizontal and vertical coordinates of the encrypted OFDM signal are derived based on color seeking of random sequences *X* and *Y* respectively.

$$R' = Seek\left(R(X' \rightarrow X)\right) \quad G' = Seek\left(G(Y' \rightarrow Y)\right) \tag{5}$$

In the next step, the OFDM signal is encrypted by transforming data blocks after cluster forming to new positions based on chaotic sequence color seeking mechanism described in (6).

$$\left[R'\left(block\right),\ G'\left(block\right)\right] = Seek\left[R\left(block\right),\ G\left(block\right)\right] \tag{6}$$

The original OFDM modulated signal with *N* subcarriers in frequency domain is denoted as $\{X_n,\quad n = 1, 2, \cdots N\}$. After cluster forming, one OFDM frame is partitioned into *M* disjoint blocks expressed as $\{X_m^b,\quad m = 1, 2, \cdots M\}$. The OFDM data after cluster forming can be described as:

$$X_n = \sum_{m=1}^{M} X_m^{\mathrm{b}} = \sum_{m=1}^{M} D(X_n), \tag{7}$$

where function *D* donates method of cluster forming related to common divisors of OFDM signal matrix size. The signal after color seeking and position relocation can be expressed as:

$$X_{en}^b = \sum_{m=1}^{M} T\left(R\left(X_m^b\right), G\left(X_m^b\right)\right), \tag{8}$$

TABLE I
COMPUTATIONAL COMPLEXITY OF THE ENCRYPTION AND DECRYPTION

	Sorting	Seeking	Total
Complexity	$O\left(\frac{L_N}{p} log \frac{L_N}{p} + \frac{L_S}{q} log \frac{L_S}{q}\right)$	$O\left(L_N * L_S\right)$	$O\left(\frac{L_N}{p} log \frac{L_N}{p} + \frac{L_S}{q} log \frac{L_S}{q} + L_N * L_S\right)$

where *T* represents the transformation of original OFDM blocks to disturbed blocks based on the color seeking mechanism. Consequently, the original OFDM signal is successfully encrypted as exhibited on the right in Fig. 2. The encrypted signal in time domain is expressed in (9).

$$\begin{aligned} x_{\mathrm{en}}^b &= IFFT \sum_{m=1}^{M} T\left(R\left(X_{\mathrm{m}}^b\right), G\ \left(X_{\mathrm{m}}^b\right)\right) \\ &= \sum_{m=1}^{M} T(R, G) \cdot\ x_m^b \end{aligned} \tag{9}$$

According to the definition of PAPR [43], the PAPR of x_{en}^b can be expressed as:

$$PAPR(x_{\mathrm{en}}^b) = 10\ \log_{10} \frac{\max\left|x_{\mathrm{en}}^b\right|^2}{E\left\{\left|x_{en}^b\right|^2\right\}}. \tag{10}$$

The PAPR value is related to the method of cluster forming *D* because the time domain encrypted signal x_m^b is derived during the process of cluster forming $x_m^b = D(x_n)$. PAPR performance can be optimized by selecting appropriate *D* to determine the cluster forming method. Through analysis and calculation, the PAPR performance of the system is optimal when the size of cluster is 2×8.

Assume that the block size is $p \times q$, the original OFDM signal consists of L_N subcarriers and L_S OFDM symbols. The computational complexity of the proposed scheme is detailed in Table I.

By using a cluster disturbance based on a chaotic sequence color seeking mechanism, the proposed encryption scheme simultaneously enhances both security and PAPR performance. At the receiving end, the signal can be decrypted and recovered using shared keys and the cluster forming method.

III. EXPERIMENTAL SETUP AND RESULTS

A. Experimental Setup

Fig. 3 illustrates the experimental diagram of the proposed CO-OFDM encryption scheme based on the chaotic sequence color seeking mechanism. At the transmitter, the transmitted data was processed offline to realize the encryption. Thereafter, the encrypted signal was used to modulate an external cavity laser (ECL) through an I/Q modulator and then transmitted over the optical fiber. At the receiver, coherent detection of the received signal and demodulation of OFDM symbols were implemented. Finally, the decrypted data was obtained after DSP and decryption operations.

In the off-line DSP, an fast Fourier transform/inverse fast Fourier transform (FFT/IFFT) size of 512 was used with 256

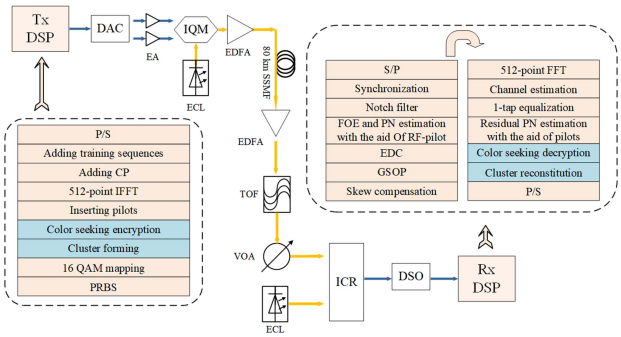

Fig. 3. Experimental setup of the proposed security enhanced CO-OFDM system over 80 km fiber. CP: Cyclic prefix, ECL: External cavity laser, DAC: Digital-to-analog converter, EA: Electrical amplifier, IQM: I/Q modulator, EDFA: Erbium doped optical fiber amplifier, SSMF: Standard single-mode fiber, TOF: Tunable optical filter, VOA: Variable optical attenuator, ICR: Integrated coherent receiver, DSO: Digital storage oscilloscope, GSOP: Gram–Schmidt orthogonalization procedure, EDC: Electronic dispersion compensation, FOE: Frequency offset, PN: Phase noise.

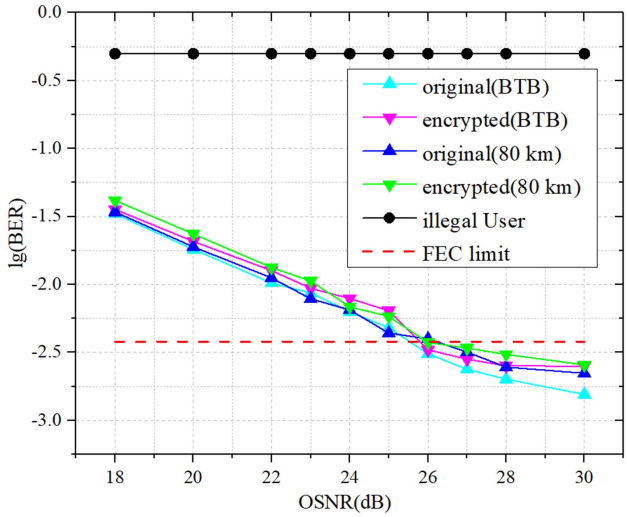

Fig. 4. BERs of the original and encrypted OFDM signals versus OSNR in the CO-OFDM system transmitted back-to-back and via 80 km of optical fiber respectively.

data-carried subcarriers, 4 pilots and 252 zero padding (ZP) at the edge of IFFT. 200 OFDM symbols with modulation format of 16QAM were generated. After performing IFFT of the encrypted data and P/S conversion, a CP with length as 1/32 of the OFDM symbol was appended to prevent inter symbol interference (ISI). Further, 20 symbols were used as training sequence to realize IQ imbalance compensation and obtain channel response. Thereafter, the encrypted OFDM signal was converted from digital to analog using an arbitrary waveform generator (AWG) with a sampling rate of 80 GSa/s. An ECL CW laser is used as the light source having central wavelength of 1550 nm. The encrypted signal from the AWG was first amplified using EA and then loaded onto the optical carrier using an IQ modulator. After removing training sequence, CP and the forward error correction (FEC) overhead, the net data rate of OFDM signals transmitted after modulation was approximately 124 Gb/s. Subsequently, the optical signal having power of 0 dBm was transmitted through an 80 km standard single-mode fiber with a total attenuation of 17 dB. At the receiving end, the optical signal with power of −6 dBm was coherently detected using a local laser in an ICR module. The linewidth of the local laser was less than 100 kHz and the frequency offset was 300 kHz. After coherent detection, the received optical signal was converted into an electrical signal and then digitized by a DSO at the sampling rate of 80 GSa/s. Following the analog-to-digital conversion, the sampled signals were processed through offline DSP. In the DSP, skew compensation was first implemented to compensate IQ timing skew. Subsequently the GSO algorithm was applied to compensate the IQ mismatch of the receiver [44]. Furthermore, the effect of chromatic dispersion was eliminated by the EDC, and frequency offset and phase noise were estimated with the aid of an RF-pilot [45]. An Adaptive Notch Filter was used to suppress the narrowband interference caused by clock leakage of the DAC at 20 GHz [46]. After the synchronization and series-parallel conversion, FFT was used to convert the signal to frequency domain where channel estimation and equalization were implemented [47]. Subsequently, the residual phase noise estimation of the signal was realized with the help of pilots. Finally, the signal was decrypted by the authorized user according to the chaotic sequence color seeking mechanism and then demapped to recover the original data.

B. *Experimental Results*

Fig. 4 shows the bit error rate (BER) curves of the original and encrypted OFDM signals versus the optical signal to noise ratio (OSNR) in the CO-OFDM system transmitted back-to-back (BTB) and via 80 km of optical fiber respectively. For the illegal user, BER maintains at approximately 0.5, which indicates that no valid information can be derived from encrypted signal. For the authorized user, when the OSNR is above 26 dB, all the BERs are below the hard-decision forward error correction (HD-FEC) limit of 3.8×10^{-3}, which indicates that the received signal can be effectively recovered.

Furthermore, in the OFDM system, PAPR is an important factor that determines the linear working area of the power amplifier and influences BER performance of system. Thus, the complementary cumulative distribution functions (CCDF) of

PAPR with and without encryption were measured in the experiment and the results are shown in Fig. 5. The results show that the encrypted OFDM signal has a PAPR that is 0.5 dB lower than the original signal, demonstrating the effectiveness of the proposed physical layer encryption scheme in enhancing PAPR performance. This optimization of PAPR performance helps to reduce the requirements for the transmitter's amplifier and DAC.

IV. Analyses of Security and PAPR Performance

The security performance of encrypted system depends on the sensitivity to initial values for keys and the randomness of chaotic sequences. Fig. 6 shows the evolution of state variable x in (1) during n times of iteration with two different initial values of key u in Brownian motion. Variable x changes dramatically as the number of iterations n increases when the initial value is changed by 10^{-15}. Other system parameters and keys in

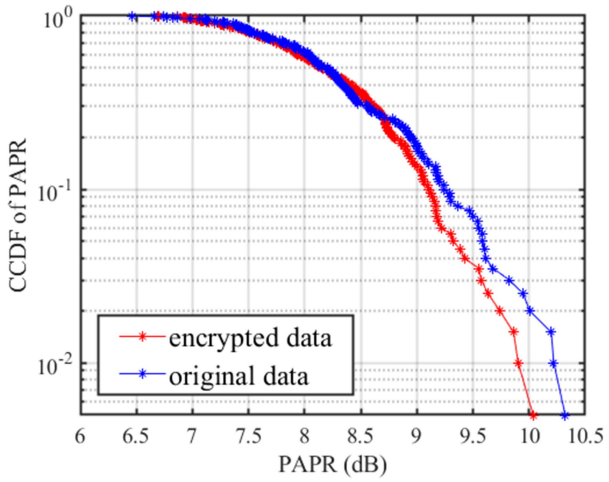

Fig. 5. Comparison of the CCDFs for the CO-OFDM signals with and without encryption.

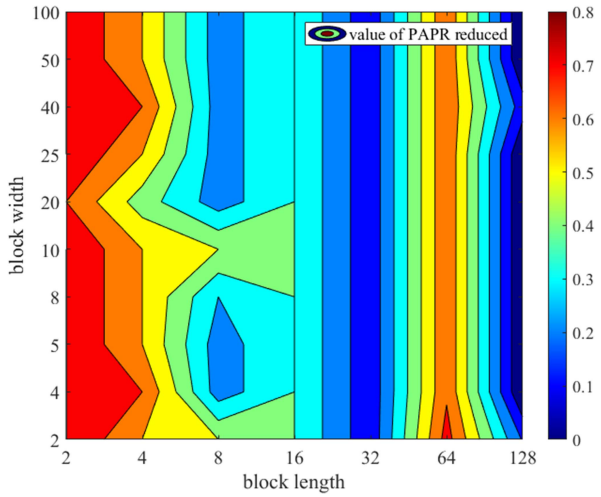

Fig. 8. The maximum values of PAPR reduced for different block sizes.

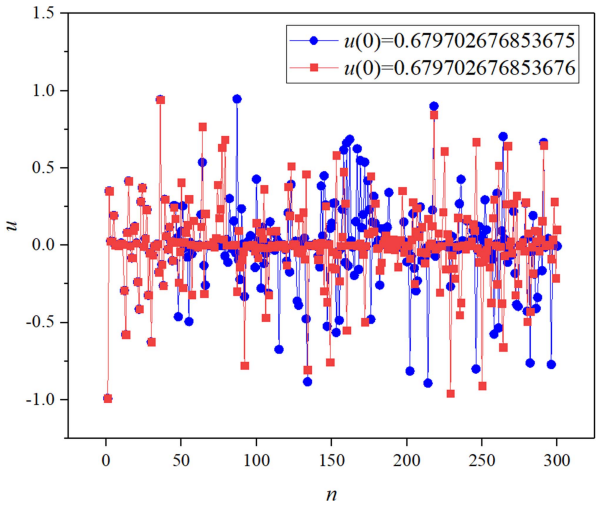

Fig. 6. Sensitivity of state variable x of Brownian motion with different initial values.

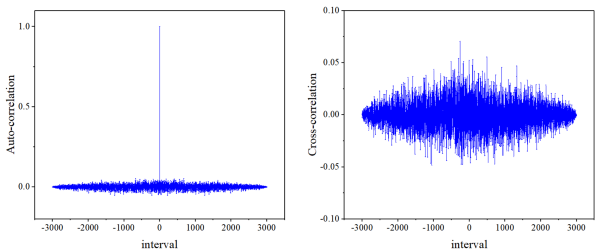

Fig. 7. Auto-correlation and cross-correlation of chaotic sequences X and X_1 generated by Brownian motion.

Brownian motion exhibit a similar characteristic, which verifies high sensitivity of Brownian motion.

Fig. 7 shows auto-correlation and cross-correlation of the two chaotic sequences X and X_1 with different initial values of key u. It illustrates that the generated chaotic sequence has good auto-correlation and cross-correlation characteristics, which effectively ensures the randomness of chaotic sequence determining the color seeking mechanism.

The key space can be calculated according to the keys used during process of color seeking mechanism encryption where keys 1–3 are system parameters and key 4–6 are initial values determining chaotic sequences in Brownian motion. Meanwhile, a and b represent the numbers of common divisor of L_N and L_S respectively after cluster forming when the size of OFDM signal matrix is $L_N \times L_S$. Therefore, the key space is $(1 \times 10^{15})^6 \times a \times b = a \times b \times 10^{90}$, which can resist brute force attacks effectively because of the tremendous time required to seek out a correct key based on existing technology.

For the proposed physical layer encryption scheme, PAPR performance of system can also be optimized during enhancement of the security performance. Cluster forming method D in (7) is an important factor that influences the value of derived PAPR. D is related to common divisors of OFDM signal matrix size. The block length can be selected from common divisors of the length of signal matrix while block width from common divisors of the width of signal matrix. The maximum values of PAPR reduced for different block sizes after cluster forming are shown in the contour map of Fig. 8 via simulation where the OFDM signal matrix size is 256 × 200. PAPR can be reduced by as much as 0.8 dB with different block sizes, resulting in significant improvements in BER performance and reduced system hardware requirements. From the results, the OFDM signal is divided into blocks with 2 × 8 size in the experiment.

Furthermore, influence of cluster forming method D on the encryption and decryption time is analyzed. A personal computer (PC) with 32 GB memory, 2.5 GHz Intel(R) Core(TM) i7-11700 and Windows 10 system is used to calculate the processing time of encryption and decryption.

The encryption and decryption time under different block sizes are shown Fig. 9. The results indicate that the encryption time is generally inversely proportional to the block size and largely affected by block width. In addition, the decryption time varies slightly with block sizes. From the time complexity perspective, it is better to select a block size with a shorter execution time when determining the cluster forming method.

Fig. 10 illustrates how encryption and decryption time change with block width when the block length is set to 2 to achieve

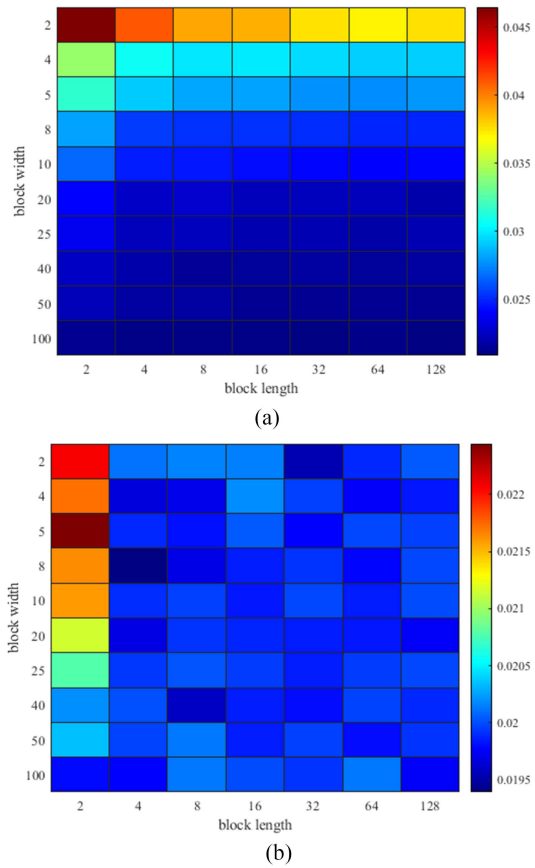

Fig. 9. The analyses of (a) encryption and (b) decryption time under different block sizes.

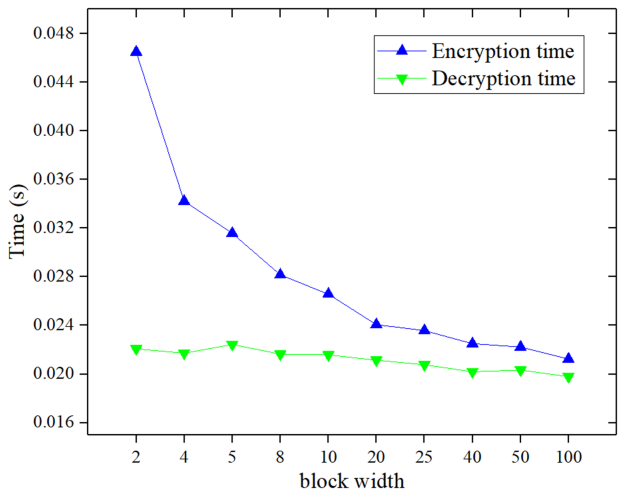

Fig. 10. The curves of encryption and decryption time with block width.

optimal PAPR. As a result, the block size is determined to be 2×8, where encryption and decryption time are minimal and the key space is relatively large. The cluster forming method is therefore dependent on a combination of encryption performance, PAPR optimization, and execution time.

In terms of key management, the computational complexity of the key sequences is calculated and presented in Table II.

TABLE II
COMPUTATIONAL COMPLEXITY OF THE KEY SEQUENCES

	Addition	Multiplication	Sorting	Total
Encryption	2L	2L	2LlogL	2L(logL+3)
Decryption	2L	2L	2LlogL	2L(logL+3)

Assuming that the number of transmitted key sequences is L and that chaotic sequences are also generated, the complexity of addition and multiplication operations both scales with L, while the complexity of the sorting operation scales with LlogL.

V. CONCLUSION

In this article, a physical layer encryption scheme for CO-OFDM system has been proposed based on disturbance of data cluster under chaotic sequence color seeking mechanism, wherein chaotic sequences are generated with a random and unpredictable Brownian motion determined by 6 keys. Randomness and scrambling performance of encryption in the system have been improved and good PAPR performance can be achieved simultaneously. An experiment was successfully implemented to demonstrate the physical layer secure transmission in a CO-OFDM system with data rate of 124 Gb/s over an 80 km SSMF. For the authorized user, information can be successfully decrypted from the received signal, while the eavesdroppers cannot derive valid information with bit error rate at approximately 0.5. Strong ability to resist brute force attacks can be provided by the scheme due to the large key space of 10^{90}. Meanwhile, PAPR is reduced by 0.5 dB during encryption through the scrambling of data cluster owing to the breakdown of the phase transition relationship between adjacent symbols. Through analyses of PAPR performance and time complexity under different cluster forming method, block size is optimized as 2×8 in the process of encryption. These results indicate that the proposed security enhancement scheme has high security and applicability in the high speed and long distance CO-OFDM systems.

REFERENCES

[1] J. Armstrong, "OFDM for optical communications," *J. Lightw. Technol.*, vol. 27, no. 3, pp. 189–204, Feb. 2009.
[2] N. Cvijetic, "OFDM for next-generation optical access networks," *J. Lightw. Technol.*, vol. 30, no. 4, pp. 384–398, Feb. 2012.
[3] I. B. Djordjevic and B. Vasic, "Orthogonal frequency division multiplexing for high-speed optical transmission," *Opt. Exp.*, vol. 14, no. 9, pp. 3767–3775, 2006.
[4] C. C. Santos and K. D. R. Assis, "Optical networks security: Design to avoid the jamming attacks," in *Proc. 13th Int. Conf. Transparent Opt. Netw.*, 2011, pp. 1–4.
[5] K. Shaneman and S. Gray, "Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention," in *Proc. IEEE Mil. Commun. Conf.*, 2004, vol. 2, pp. 711–716.
[6] M. Furdek and N. Skorin-Kapov, "Physical-layer attacks in all-optical WDM networks," in *Proc. 34th Int. Conv. MIPRO*, 2011, pp. 446–451.
[7] A. Maslo, N. Sarajlić, M. Hodžić, and A. Mujčić, "Optical network security attacks by tapping and encrypting optical signals," in *Adv. Technol., Syst., Appl. V*, Ed., Springer, 2021, pp. 321–332. [Online]. Available: https://link.springer.com/book/10.1007/978-3-030-54765-3
[8] B. Wu, B. J. Shastri, and P. R. Prucnal, "Secure communication in fiber-optic networks," in *Emerging Trends in ICT Security*. Burlington, MA, USA: Morgan Kaufmann, 2014, pp. 173–183.

[9] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 725–736, Sep. 2011.
[10] C. Huang, P. Y. Ma, B. J. Shastri, P. Mittal, and P. R. Prucnal, "Robustness of optical steganographic communication under coherent detection attack," *IEEE Photon. Technol. Lett.*, vol. 31, no. 4, pp. 327–330, Feb. 2019.
[11] Z. Wang, L. Xu, J. Chang, T. Wang, and P. R. Prucnal, "Secure optical transmission in a point-to-point link with encrypted CDMA codes," *IEEE Photon. Technol. Lett.*, vol. 22, no. 19, pp. 1410–1412, Oct. 2010.
[12] Y. Xiao, L. Zhou, Z. Pan, Y. Cao, and W. Chen, "Physically-enhanced ghost encoding," *Opt. Lett.*, vol. 47, no. 2, pp. 433–436, 2022.
[13] L. Liu et al., "Physical layer encryption scheme based on cellular automata and DNA encoding by hyper-chaos in a CO-OFDM system," *Opt. Exp.*, vol. 29, no. 12, pp. 18976–18987, 2021.
[14] B. Wu, Y. Tang, C. Qiu, Y. Huang, C. Huang, and P. R. Prucnal, "Secure analysis of optical steganography with spectral signature measurement," *IEEE Photon. Technol. Lett.*, vol. 33, no. 17, pp. 971–974, Sep. 2021.
[15] P. Y. Ma, B. Wu, B. J. Shastri, A. N. Tait, P. Mittal, and P. R. Prucnal, "Steganographic communication via spread optical noise: A link-level eavesdropping resilient system," *J. Lightw. Technol.*, vol. 36, no. 23, pp. 5344–5357, Dec. 2018.
[16] Y. Huang et al., "Temporal and spectral coding over amplified spontaneous emission for secure optical coherent communications," *Opt. Lett.*, vol. 45, no. 4, pp. 1039–1042, 2020.
[17] 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.
[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] Z. Gao et al., "32 Gb/s physical-layer secure optical communication over 200/km based on temporal dispersion and self-feedback phase encryption," *Opt. Lett.*, vol. 47, no. 4, pp. 913–916, 2022.
[20] A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, "Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling," *J. Lightw. Technol.*, vol. 39, no. 8, pp. 2288–2295, Apr. 2021.
[21] N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, pp. 1536–1539, 2019.
[22] A. Sultan, X. Yang, A. A. E. 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.
[23] Y. Wu et al., "60 Gb/s coherent optical secure communication over 100/km with hybrid chaotic encryption using one dual-polarization IQ modulator," *Opt. Lett.*, vol. 47, no. 20, pp. 5285–5288, 2022.
[24] C. Gao et al., "Physical layer encryption for polarization division multiplexing coherent optical communication system based on the rotation of the state of polarization," in *Proc. 19th Int. Conf. Opt. Commun. Netw.*, 2021, pp. 1–3.
[25] X. Liang, C. Zhang, Y. Luo, X. Wang, and K. Qiu, "Secure encryption and key management for OFDM-PON based on chaotic Hilbert motion," *J. Lightw. Technol.*, vol. 41, no. 6, pp. 1619–1625, Mar. 2023.
[26] X. Liang, C. Zhang, Y. Luo, M. Cui, and K. Qiu, "Secure key distribution and synchronization method in an OFDM-PON based on chaos," *Opt. Exp.*, vol. 30, no. 11, pp. 18310–18319, 2022.
[27] Z. Yang, J. Ke, Q. Zhuge, W. Hu, and L. Yi, "Coherent chaotic optical communication of 30 Gb/s over 340-km fiber transmission via deep learning," *Opt. Lett.*, vol. 47, no. 11, pp. 2650–2653, 2022.
[28] L. Jiang et al., "Trading off security and practicability to explore high-speed and long-haul chaotic optical communication," *Opt. Exp.*, vol. 29, no. 8, pp. 12750–12762, 2021.
[29] X. Tang et al., "A physical layer security-enhanced scheme in CO-OFDM system based on CIJS encryption and 3D-LSCM Chaos," *J. Lightw. Technol.*, vol. 40, no. 12, pp. 3567–3575, Jun. 2022.
[30] 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.
[31] K. Zhang, J. Zhang, G. Gao, and A. Fei, "Physical layer security based on chaotic spatial symbol transforming in fiber-optic systems," *IEEE Photon. J.*, vol. 10, no. 3, Jun. 2018, Art. no. 7202410.
[32] Y. Wan et al., "Secure OFDM transmission scheme based on chaotic encryption and noise-masking key distribution," *Opt. Lett.*, vol. 47, no. 11, pp. 2903–2906, 2022.
[33] J. Zhao et al., "High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization," *Opt. Exp.*, vol. 28, no. 14, pp. 21236–21246, 2020.
[34] L. Yuan et al., "High-security OCDM-PON system of 7-core fiber based on CFCM encryption," *Opt. Lett.*, vol. 47, no. 1, pp. 186–189, 2022.
[35] X. Song et al., "SCMA-OFDM PON based on chaotic-SLM-PTS algorithms with degraded PAPR for improving network security," *Opt. Lett.*, vol. 47, no. 20, pp. 5293–5296, 2022.
[36] S. Chen et al., "A 7D cellular neural network based OQAM-FBMC encryption scheme for seven core fiber," *J. Lightw. Technol.*, vol. 39, no. 22, pp. 7191–7198, Nov. 2021.
[37] 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. 2018.
[38] L. Jiang et al., "Chaotic optical communications at 56 Gbit/s over 100-km fiber transmission based on a chaos generation model driven by long short-term memory networks," *Opt. Lett.*, vol. 47, no. 10, pp. 2382–2385, 2022.
[39] 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.
[40] 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. Exp.*, vol. 27, no. 20, pp. 27946–27961, 2019.
[41] T. Wu et al., "Security enhancement for OFDM-PON using Brownian motion and chaos in cell," *Opt. Exp.*, vol. 26, no. 18, pp. 22857–22865, 2018.
[42] W. Zhang, C. Zhang, C. Chen, H. Zhang, and K. Qiu, "Brownian motion encryption for physical-layer security improvement in CO-OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 12, pp. 1023–1026, Jun. 2017.
[43] T. Jiang and Y. Wu, "An overview: Peak-to-average power ratio reduction techniques for OFDM signals," *IEEE Trans. Broadcast.*, vol. 54, no. 2, pp. 257–268, Jun. 2008.
[44] H. S. Chung, S. H. Chang, and K. Kim, "Effect of IQ mismatch compensation in an optical coherent OFDM receiver," *IEEE Photon. Technol. Lett.*, vol. 22, no. 5, pp. 308–310, Mar. 2010.
[45] S. L. Jansen, I. Morita, T. C. W. Schenk, N. Takeda, and H. Tanaka, "Coherent optical 25.8-Gb/s OFDM transmission over 4160-km SSMF," *J. Lightw. Technol.*, vol. 26, no. 1, pp. 6–15, Jan. 2008.
[46] F. Li et al., "100 Gbit/s PAM4 signal transmission and reception for 2-km interconnect with adaptive notch filter for narrowband interference," *Opt. Exp.*, vol. 26, no. 18, pp. 24066–24074, 2018.
[47] T.-H. Nguyen et al., "Experimental demonstration of the tradeoff between chromatic dispersion and phase noise compensation in optical FBMC/OQAM communication systems," *J. Lightw. Technol.*, vol. 37, no. 17, pp. 4340–4348, Sep. 2019.

Le Liu received the B.S. degree from Xi'an University of Posts and Telecommunications, Xi'an, China, in 2019. He is currently working toward the Ph.D. degree with the Beijing University of Posts and Telecommunications, Beijing, China. His research interests include optical secure transmission and optical secure key distribution.

Xianfeng Tang received the Ph.D. degree in physical electronics from the Beijing University of Posts and Telecommunications, Beijing, China, in 2011. He is currently an Associate Professor with the School of Electronic Engineering, Beijing University of Posts and Telecommunications. He is also the author of several patents and more than 70 papers in top journals and conferences. He has authored or coauthored two books and translated the book of Optics by Prof. Ajoy Ghatak. His research interests include optical secure transmission, high-speed optical fiber communication, and optical information processing.

Fan Li biography is not available at the time of publication.

Zeyu Xu received the B.S. degree in 2022 from the Beijing University of Posts and Telecommunications, Beijing, China, where he is currently working toward the M.S. degree. His research interests include optical secure transmission and high-speed optical fiber communication.

Xiaoguang Zhang biography is not available at the time of publication.