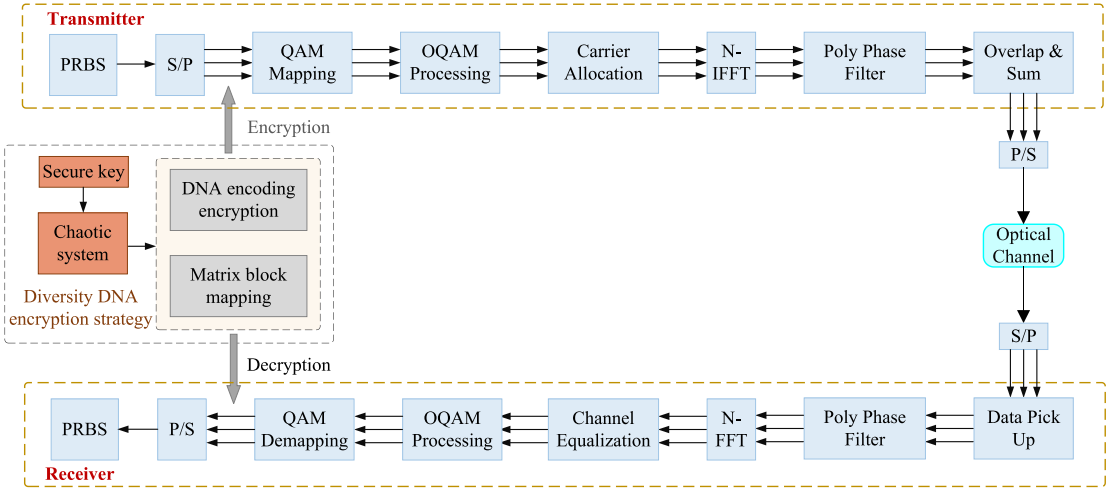
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

FBMC/OQAM Security Strategy Based on Diversity DNA Encryption

Volume 13, Number 1, February 2021

Rong Tang
Bo Liu
Jianxin Ren
Yaya Mao
Jianye Zhao
Shun Han
Yang Han
Shuaidong Chen



DOI: 10.1109/JPHOT.2021.3054529

FBMC/OQAM Security Strategy Based on Diversity DNA Encryption

Rong Tang,[1] Bo Liu,[1] Jianxin Ren,[2] Yaya Mao,[1] Jianye Zhao,[1] Shun Han,[1] Yang Han,[1] and Shuaidong Chen[1]

[1]Institute of Optics and Electronics, Nanjing University of Information Science and Technology, Nanjing 210044, China
[2]School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

DOI:10.1109/JPHOT.2021.3054529

Manuscript received December 23, 2020; revised January 19, 2021; accepted January 22, 2021. Date of publication January 26, 2021; date of current version February 17, 2021. This work was supported in part by the financial support from National Key Research and Development Program of China under Grant 2018YFB1801302, in part by the National Natural Science Foundation of China under Grants 61835005, 61822507, 61675004, 61705107, 61775098, 61727817, 61720106015, 61875248, 61975084, 61935011, and 61935005, in part by Open Fund of IPOC (BUPT), in part by Jiangsu talent of innovation and entrepreneurship, and in part by Jiangsu team of innovation and entrepreneurship.
Corresponding author: Bo Liu (e-mail: bo@nuist.edu.cn).

Abstract: In this paper, a diversity deoxyribonucleic acid (DNA) chaotic encryption strategy is proposed to enhance the physical layer security of the filter bank multi-carrier/offset quadrature amplitude (FBMC/OQAM) system. After the input original binary bit stream is encrypted, it is subjected to FBMC/OQAM modulation. The encryption process of bit data is dynamically controlled by the chaotic sequences generated by the hybrid chaotic system composed of improved-Logistic and delayed tent sine system, which enhances the robustness against malicious attacks by illegal attackers. The diversity DNA encryption strategy expands the key space of the system to 10^{180}, which can ensure the physical layer security of the system. The proposed FBMC/OQAM security strategy based on chaotic encryption is transmitted on 25 km standard single mode fiber. Experimental results show that the diversity DNA encryption strategy can effectively ensure the security of transmitted data.

Index Terms: Diversity DNA encryption, physical layer security, FBMC/OQAM, chaotic system.

1. Introduction

Multi-carrier modulation (MCM) has become a key physical layer transmission technology in communication systems, because it can effectively deal with frequency selective channels and transmit data at high bit rates on multiple parallel sub-channels. As one of the most important technologies in MCM, orthogonal frequency division multiplexing (OFDM) has been widely studied due to its high robustness to multipath effects and high bandwidth efficiency. However, due to the large sidelobes, the OFDM system is susceptible to inter-carrier crosstalk, and cyclic prefix (CP) needs to be added to reduce interference, which will bring additional overhead and loss of spectrum efficiency to the system [1]–[3]. The filter bank multicarrier/offset quadrature-amplitude (FBMC/OQAM) modulation technology is designed with a proper prototype filter, which eliminates the need to introduce CP and guard intervals in the system. In addition, FBMC has the advantages

of robustness against narrowband interference and lower sidelobes, as a non-CP-OFDM system, FBMC/OQAM achieves the high spectral efficiency [4]–[8]. And with the development of digital filtering technology, FBMC/OQAM will play a huge role in the next generation communication system. However, as a multi-carrier system, some very challenging problems need to be solved when designing the FBMC/OQAM system, such as the high peak-to-average power ratio (PAPR) of the transmitted signal [9]–[11]. In order to make full use of the advantages of FBMC/OQAM technology, it is very important and necessary that the proposed physical layer encryption scheme cannot cause damage to the system.

In addition to the research on improving the performance of the communication system itself, the security of the system has also been a hot research topic in recent years. Among the existing security schemes, encryption schemes based on chaotic systems are widely used in the fields of electronics [12] and optical signals [13] because of their pseudo-randomness, high sensitivity to initial values and ergodicity. Compared with the encryption technology in the optical field, including simulated optical chaos [14] and exclusive OR (XOR) interference [15], the chaotic encryption scheme that uses digital signal processing (DSP) processing in the electronic domain does not require additional optical components, which effectively reduces the system cost. So, the electronic domain encryption scheme based on chaos has been widely studied, such as constellation encryption [16]–[18], symbol and subcarrier scrambling [19]–[22], etc., these methods can obtain a huge key space and effectively guarantee the security of the system, but the use of a single chaotic system for signal encryption increases the risk of statistical analysis attacks. Deoxyribonucleic acid (DNA) encoding has the advantages of strong parallelism and large storage capacity, chaotic DNA encoding can enhance the security of information, and is widely used in image encryption [23]–[25]. Zhang et al. proposed an orthogonal frequency division multiplexing passive optical network (OFDM-PON) encryption system based on DNA encryption [26], which can increase the complexity and randomness of chaotic encryption sequences and improve the physical layer security of the system. The typical DNA encryption methods can be improved to increase the key space, make brute force cracking more difficult, and further guarantee the physical layer security of the communication system.

On the basis of research on existing encryption methods, a diversity DNA chaotic encryption strategy is proposed for the first time in this paper. Uses improved-Logistic and delayed tent sine (DTS) hybrid chaotic system to generate chaotic sequences, and control the encryption steps. Expanding the DNA encode to 3 bits, which can enlarge the key space to 10^{180}, while effectively resist malicious attacks, improving the security of the physical layer of communication system. After diversity DNA encryption are performed on the original binary data, it is modulated to generate FBMC/OQAM data. The DNA diversity rules, binary and base encoding/decoding rules, key base sequence and DNA base sequence scrambling rules are controlled by different chaotic sequences. The FBMC/OQAM security system proposed in this paper has been experimentally verified using 25 km standard single mode fiber (SSMF). The results show that the proposed diversity DNA chaotic encryption strategy can effectively improve the physical layer security of the transmission system, effectively resist illegal receivers, and improve the security of the FBMC/OQAM system without destroying the PAPR performance of the signal.

2. Principle of FBMC/OQAM Security Strategy Based on Diversity DNA Encryption

The principle of the diversity DNA chaotic encryption strategy is shown in the Fig. 1. In the transmitter of the FBMC/OQAM system, the pseudo-random binary sequence (PRBS) generated by the DSP is used as the original input data.

Firstly, perform serial/parallel (S/P) conversion of the PRBS to generate a matrix. Every three elements in the matrix are divided into a group to form $N/31\times3$ row vector blocks, where N is the number of bits in PRBS. After selecting one of these row vector blocks as the starting block, these row vector blocks are mapped according to the specified rule to form a new matrix. Then encode the

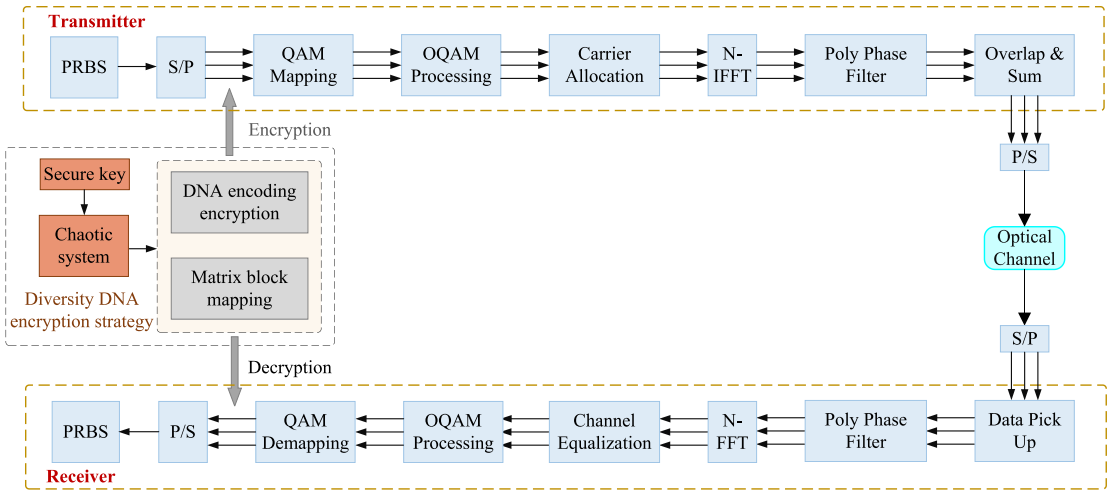


Fig. 1. The principle of the FBMC/OQAM security strategy of diversity DNA chaotic encryption.

mapped data into base sequences according to the DNA encoding rules, two different encoding rules are used, and the base sequence is encrypted based on the chaotic scrambling method. There are three scrambling rules, namely addition, subtraction and XOR, chaotic sequences are used to select specific rules for base scrambling. After the above steps are completed, the scrambled base sequence is restored to a binary sequence through base-binary conversion, and data encryption is completed at this time. The encrypted signal is converted into S/P and modulated into FBMC/OQAM data for transmission. The chaotic sequences control every step in the data encryption process. Only the receiver with the correct chaotic initial values and DNA encryption rules can obtain the original information from the ciphertext using the calculation method opposite to that of the transmitter.

Use DTS chaotic system to generate chaotic sequences K_1, K_2, K_3, K_4, DTS algorithm is expressed as:

$$\begin{aligned} x_{i+1} &= \sin(\pi(T(r, x_{i-m}))) + S(1-r, x_{i-m}) \\ &= \begin{cases} \sin(\pi(2rx_{i-m} + Q)) & x_i < 0.5 \\ \sin(\pi(2r(1-x_{i-m}) + Q)) & x_i \geq 0.5 \end{cases} \\ Q &= (1-r)\sin(\pi x_{i-m}) \end{aligned} \tag{1}$$

where $m = 1, 2, \ldots, 8$ is the delay number, and the bifurcation parameter $r = 0.26$. The chaotic sequences are obtained by the following calculation:

$$\begin{aligned} K_1 &= ceil(\mathrm{mod}((DTS(x, m)) \times 10^5, 2) - 1), && m = 2 \\ K_2 &= ceil(\mathrm{mod}((DTS(x, m)) \times 10^5, 2) - 1), && m = 3 \\ K_3 &= \mathrm{mod}(ceil(DTS(x, m)) \times 10^5, 3) + 1, && m = 2 \\ K_4 &= ceil(\mathrm{mod}((DTS(x, m)) \times 10^5, 2)), && m = 3 \end{aligned} \tag{2}$$

The *ceil*() function is to round the number towards positive infinity, and *mod*() is the modulo operation. According to the above calculation, the chaotic sequences K_1, K_2, K_3, K_4 can be obtained. The binary chaotic sequence L_X generated by the improved-Logistic chaotic algorithm is encoded into a key base sequence. The improved-Logistic algorithm is expressed as:

$$\begin{cases} x_{n+1} = \mu x(1-x) & x < 0.5 \\ x_{n+1} = \mu x(1-x) + {}^{\mu}/_{4} & x \geq 0.5 \end{cases} \tag{3}$$

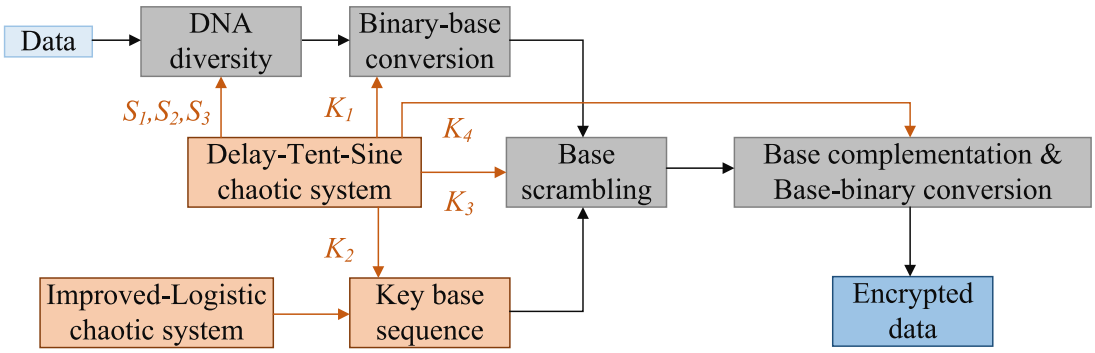


Fig. 2. DNA diversity encryption strategy process.

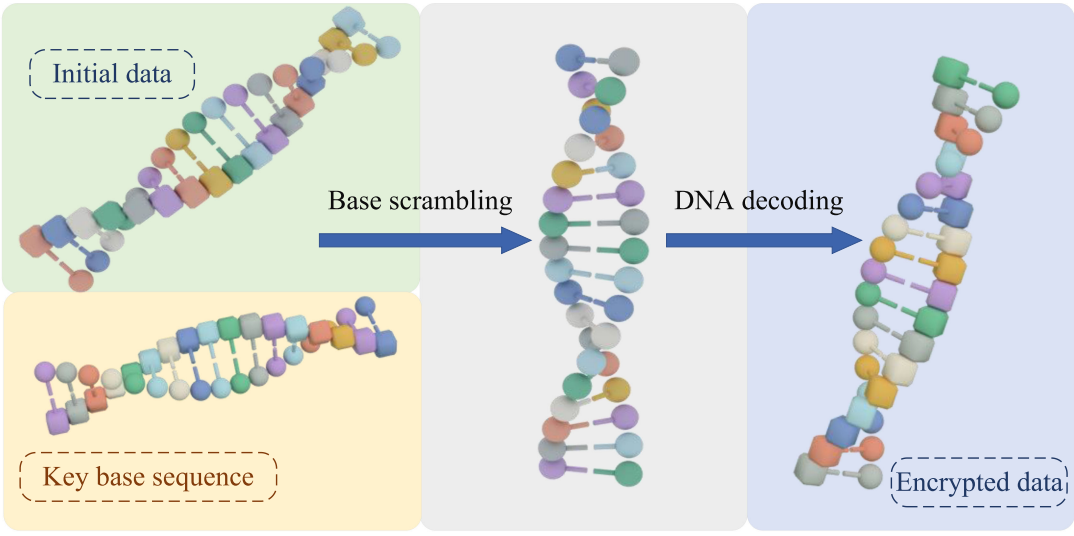


Fig. 3. Diversity DNA encryption schematic diagram.

where the initial value $x \in (01)$, the bifurcation parameter $\mu = 3.61234$.

The diversity DNA encryption process is shown in the Fig. 2, which are the DNA diversity, binary-base encoding, key base sequence generation, base scrambling, base complementary and decoding into binary symbols. Use the DTS chaotic system to generate four chaotic sequences K_1, K_2, K_3, K_4, and control the four steps of the above encryption process respectively.

Fig. 3 is the schematic diagram of diversity DNA encryption strategy. The cube represents '*0-1*' bit row vector block, and the sphere is the base. The initial data is encoded as bases after DNA diversity mapping, and then scrambled with key base sequence. The encrypted bases are decoded into bit stream to complete DNA diversity encryption finally.

Denote the binary data matrix after S/P as D, the size is $h \times p$, use sequence L_X to generate the sequences S_1, S_2 and S_3, which are used to select the initial row vector block and the DNA diversity mapping rules. The calculation process of S_1, S_2 and S_3 is expressed as:

$$S_1 = H \cdot \frac{1}{sort(L_X)^T} \cdot L_X, H = [1, 2, \ldots, h]$$

$$S_2 = P \cdot \frac{1}{sort(L_X)^T} \cdot L_X, P = [1, 2, \ldots, p]$$

$$S_3 = \mathrm{mod}((L_X) \times 10^5, 4) + 1, \quad (4)$$

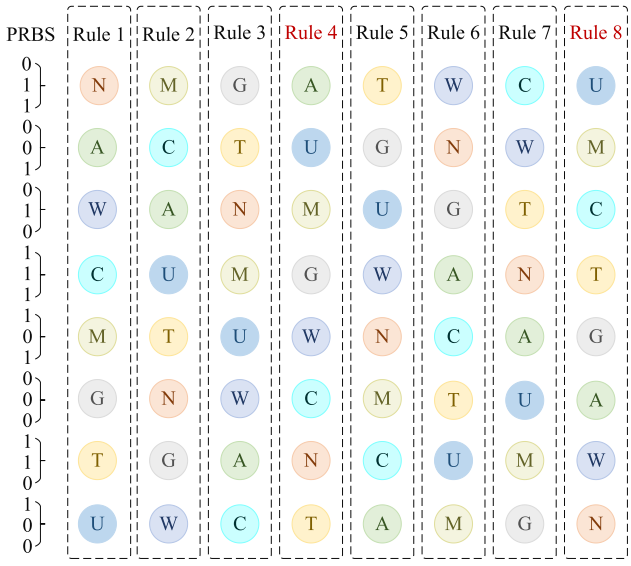


Fig. 4. Binary and base encoding rules.

sort $(L_X)^T$ is to arrange the sequence L_X in ascending order and transpose it. The calculated value ranges of the S_1 and S_2 sequences are integers in *1-h* and *1-p*, respectively. Use sequences S_1 and S_2 to determine the coordinate d_1 of the initial row vector block. Denote the selected *i*th element in S_1 and S_2 as S_1_i and S_2_i, then the coordinate d_1 is (S_1_i, S_2_i).

Starting from the initial position d_1, there are four mapping rules, which are clockwise/ counter-clockwise from the top/ bottom of d_1. Select the *i*th element in the chaotic sequence S_3, and the relationship between the value of this element and the mapping rule is: 1 means clockwise direction above S_1, 2 means counterclockwise direction above S_1, 3 means clockwise direction below S_1, 4 means counterclockwise direction below S_1. And they are all mapped in an *S*-shaped path.

After mapping all the blocks above or below the selected block, return to the selected block, and map all the blocks in matrix *D* according to the rule. The DNA diversity mapping is completed at this time, the new matrix after diversity is denoted as *D*'.

The typical DNA sequence consists of four bases: adenine (A), guanine (G), cytosine (C), and thymine (T). According to the Watson-Crick principle, the base complementary pairing rules are: A-T and C-G. Typical DNA encryption involves encoding two binary bits as one DNA base, that is, 00, 01, 10, and 11 are used to encode bases A, G, C, and T respectively. So there are $4! = 24$ encoding rules. The diversity DNA encryption strategy proposed in this paper is extended to 3 bits, and adds four additional bases on the basis of the typical DNA sequence, named M, W, U, N, the base complementary pairing rules are: M-W, U-N. Encoding three binary bits as one DNA base, based on this method, there are $8! = 40320$ encoding rules.

However, in binary encoding, 0 and 1 complement each other. Select the rules suitable for this complementary relationship from 8! kinds of encoding rules, Fig. 4 shows the alternative rules. Rules 4 and 8 are selected for encoding in this article.

Each row vector block in the matrix *D*' is completed as a group, and each group has 3 binary numbers, the rule of binary base encoding for each group is controlled by the chaotic sequence K_1. When the *i*th element of K_1 is 1, select rule 4 to encode the *i*th group of binary numbers, otherwise it is rule 8, as shown in Fig. 4. Mark the encoded base sequence as K_S.

Encode the sequence L_X to the key base chain K_B in the same method for the next base scrambling, where the selection of the encoding rule is controlled by K_2. When the *i*th element of K_2 is 1, the selection rule 4 encodes the *i*th group of L_X as base, otherwise it is rule 8.

The chaotic sequence K_3 is used to control the scrambling rules of the base sequence K_S and the base key chain K_B to obtain a new base sequence. Use three different rules to scramble the

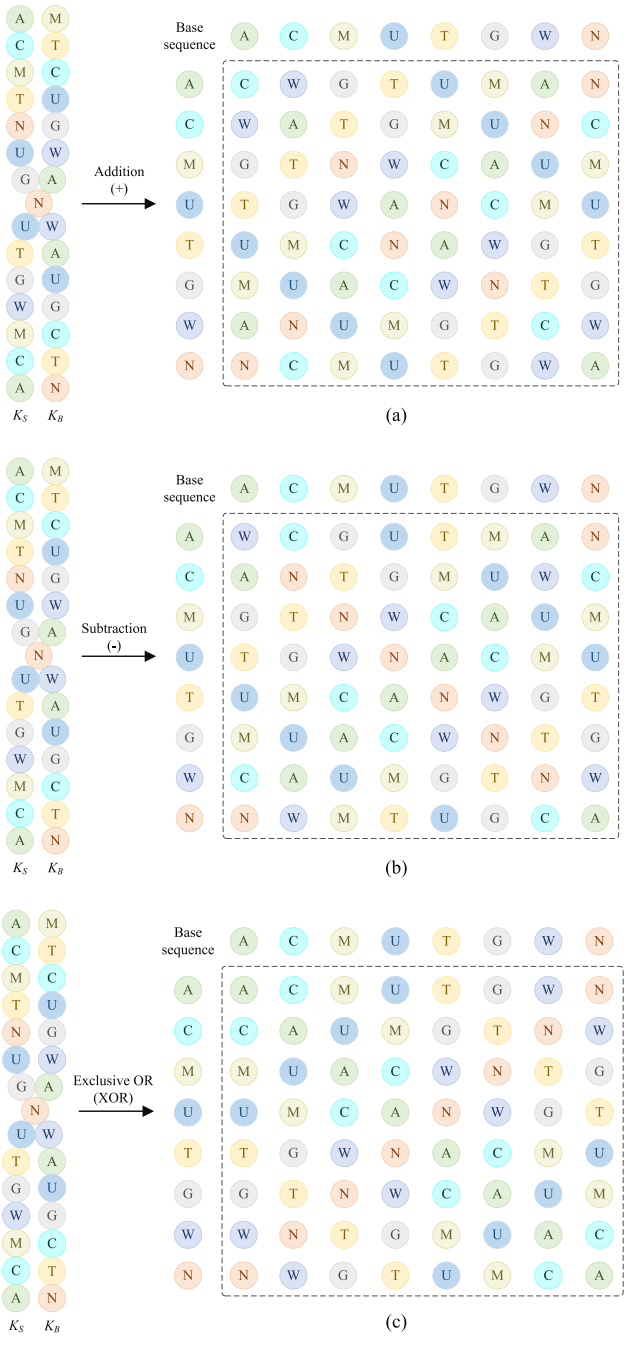


Fig. 5. Scrambling rules of base sequences. (a) addition (b) subtraction (c) exclusive OR.

bases, including addition, subtraction and XOR, the specific rules are shown in Fig. 5. As the value of the chaotic sequence K_3 changes, the base scrambling rules of each selected will also change. When the ith element of K_3 is 1, the ith pair of K_S and K_B is selected to perform addition operation, subtraction is performed when the element is 2, and XOR is selected when the element is 3.

In order to avoid the generation of continuous bases, the scrambled base is subjected to complementary operations and then decoded into binary sequences. The complement and decoding rules are controlled by the chaotic sequence K_4. When the ith element of K_4 is 1, swap the ith scrambled

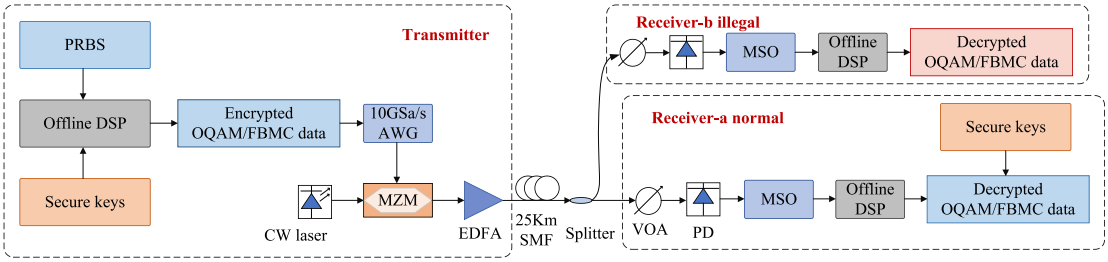


Fig. 6. Experimental setup (CW: continuous wave laser; MZM: Mach-Zehnder Modulator; AWG: arbitrary waveform generator (TekAWG70002A); SSMF: standard-single mode fiber; VOA: variable optical attenuator; PD: photo-diode; MSO: mixed signal oscilloscope (TekMSO73304DX)).

base with its complementary base, that is, swap A-T, C-G, M-W, U-N, and then select rule 4 from Fig. 4 to decode base into binary sequence, otherwise keep the base unchanged and select rule 8 to decode base into binary number. After the diversity DNA encryption is completed, the encrypted binary sequence is modulated by FBMC/OQAM and transmitted through the optical fiber link.

The size of the key space of a chaotic system directly affects whether the system can effectively resist malicious attacks. The larger the key space, the stronger the ability to resist malicious attacks. The diversity DNA encryption strategy can choose kinds of encryption rules in this paper, which expands the key space by 48 times compared with typical DNA encryption, further reducing the possibility of information being cracked by force. Use hybrid chaos system to obtain 8 chaotic sequences, of which 3 sequences are used to control the DNA diversity process, and 5 sequences are used to control the DNA scrambling process. And the key space of this method includes the initial value x, parameters r, m and μ, therefore, the system can provide a key space of $(10^{15})^4 \times (10^{15})^8 = 10^{180}$, which is sufficient to resist brute force attacks by illegal attackers.

A dynamic encryption method is used in diversity DNA encryption strategy, which must use chaotic sequences generated by chaotic system to control each encryption step. Compared with the fixed DNA encryption, using the dynamic encryption method based on chaotic system, the illegal receiver needs to break all coding rules to decrypt the ciphertext, which greatly reduces the possibility of leakage of the original information. The initial value, bifurcation parameter and delay number of the DTS and improved-Logistic system are the security keys. After the normal receiver obtains the chaotic sequences by using the security key, decryption can be performed by the reverse process of encryption, and the transmitter and the normal receiver share the security key.

3. Experiment Setup and Results

The experimental setup of the FBMC/OQAM system based on diversity DNA encryption is shown in Fig. 6. In order to test and verify the feasibility of the encryption scheme proposed in the article, a normal receiver and an illegal receiver are set up, the normal receiver has the security key, and the illegal receiver does not have the security key and can only perform brute force cracking. In the transmitter, the MATLAB program is used for offline DSP to generate encrypted FBMC/OQAM electrical signals. The number of subcarriers is set to 150, the number of symbols is 100, and the IFFT/FFT size is 512 In the experiment. The FBMC/OQAM system adopts 16-OQAM modulation and a prototype filter based on PHYDYAS filter [27] with an overlap factor of $O = 4$. Use an AWG with a sampling rate of 10 GSa/s to convert the encrypted data into an analog radio frequency (RF) signal, and then use MZM to load the RF signal onto a continuous optical carrier generated by a tunable light source. The optical transmitter uses intensity modulation for direct detection. The intensity modulator is used to modulate the optical carrier with a wavelength of 1550 nm generated by the light source, and at the same time realize the electrical-optical conversion, and then enter the SSMF of 25 km for transmission. Use EDFA at the receiver to amplify the modulated optical signal,

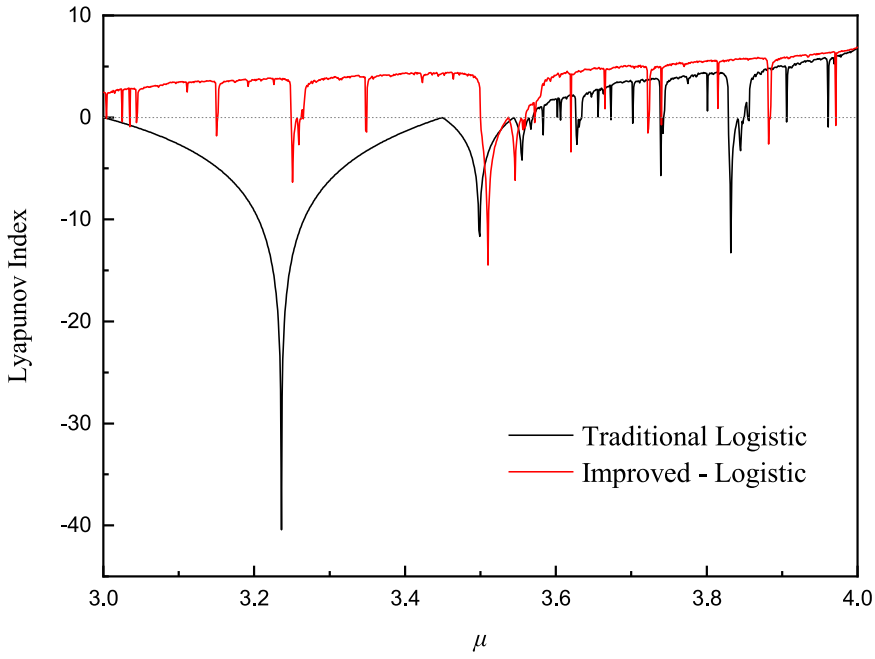


Fig. 7. The Lyapunov exponential distribution of traditional and improved-Logistic mapping algorithm under the control of different bifurcation parameters.

and then use a VOA to adjust the power of the optical signal, the received optical signal is converted into an electrical signal by a PD, and then passed through the MSO at a sampling rate of 50 GS/s, and at the same time, the analog-to-digital conversion is realized. The original transmission signal can be obtained by DNA decoding of the obtained electric signal, and the processing of the electric signal is performed offline in MATLAB.

The Lyapunov exponent is an important parameter to describe chaotic phenomena. It has been proved that for discrete dynamic systems or nonlinear time series, as long as the maximum value of the Lyapunov exponent is greater than zero, the system is chaotic [28]. And the larger the Lyapunov exponent, the more obvious the chaotic characteristics of the system.

The Fig. 7 shows the Lyapunov exponential distribution diagrams of the traditional logistic mapping and the improved-Logistic mapping algorithm under the control of different bifurcation parameters μ. It can be seen that the improved-Logistic chaotic map has a larger Lyapunov exponent than the traditional logistic chaotic map, and the bifurcation parameter μ has a larger value range, which increases the key space and improves the security of the system.

Fig. 8 shows the chaotic sequences obtained by slightly changing the initial value x in the traditional and improved-Logistic chaotic algorithm. Compared with the traditional Logistic chaotic algorithm, the improved-Logistic algorithm is more sensitive to the initial value, which more satisfies the need for the sensitivity of the chaotic system to the initial value, and the chaotic sequence value distribution obtained by the improved-Logistic chaotic algorithm is more uniform.

Fig. 9 shows the bit error rate (BER) curve and constellation diagram of normal receiver and illegal receiver after receiving and decoding. The normal receiver uses the security key can correctly decrypt the ciphertext to obtain the original information. It can be seen from the figure that for the normal receiver, when the received optical power is greater than -22 dBm, the BER is less than 10^{-3}. The illegal receiver has an BER of around 0.5, which greatly exceeds the forward error correction threshold. This shows that the diversity DNA chaotic encryption strategy can effectively protect the security of transmitted information, resist eavesdropping by illegal receivers, and the intruder cannot decipher any useful information from the ciphertext.

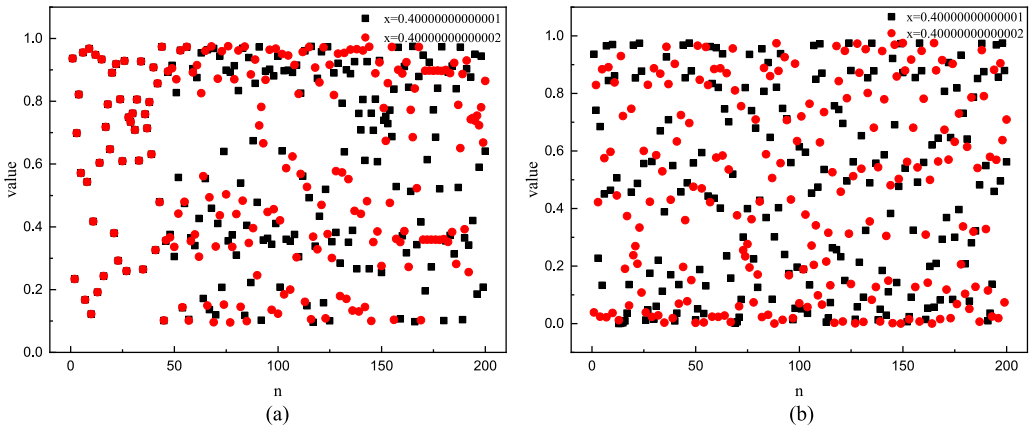


Fig. 8. The traditional and improved-Logistic chaotic sequence after minor changes to the initial value. (a). traditional logistic chaotic sequence (b). improved - Logistic chaotic sequence.

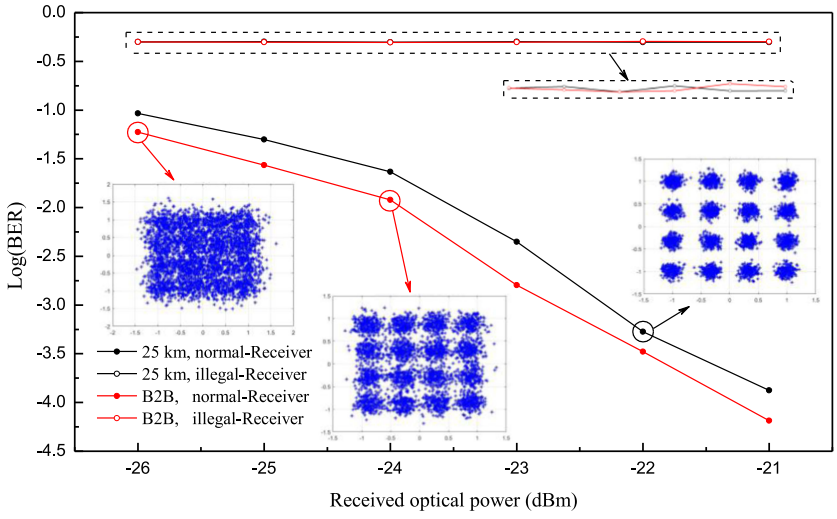


Fig. 9. BER curves of normal and illegal receivers.

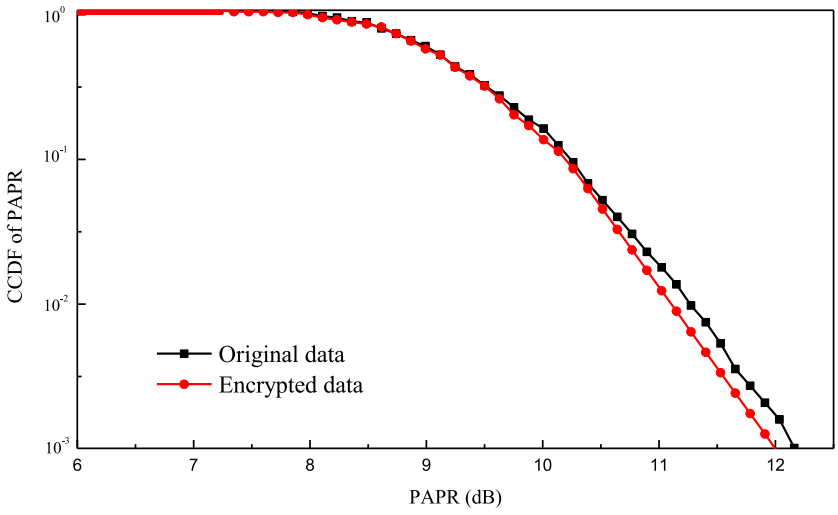


Fig. 10. PAPR and CCDF curves of encrypted and original information.

The impact of the encryption strategy mentioned in this article on PAPR is studied at the last. In Fig. 10, the red and black curves are the PAPR and complementary cumulative distribution function (CCDF) curves of the encrypted information and the original information respectively. It can be seen that the FBMC/OQAM signal after encryption has a similar trend to the original signal curve, the PAPR of the two FBMC/OQAM signals is not much different, and the PAPR performance of the encrypted signal is slightly improved compared to the original signal, which proves that the encryption strategy proposed in this article has a beneficial effect on the performance of the FBMC/OQAM system.

4. Conclusion

This paper introduces a diversity DNA chaotic encryption strategy to enhance the physical layer security of the FBMC/OQAM system. After diversity DNA encryption is performed on the initial binary bit data, the encrypted binary data is subjected to FBMC/OQAM modulation. Use improved-Logistic and DTS double chaos system to control the encryption process, which can effectively resist brute force attacks while improving the encryption performance of the system. Since only the original bit stream is encrypted, the encryption scheme is very adaptable and can be applied to communication systems that use different modulation formats. The proposed physical layer security system is verified by experiments, and it is transmitted through 25 km SSMF. The results show that the encryption strategy can expand the key space of the system to 10^{180}, effectively prevent eavesdropping, and has high sensitivity and security. At the same time, this encryption method has good BER performance in transmission, has a certain beneficial effect on the PAPR of the FBMC/OQAM system, and can be an excellent candidate to meet the high-security FBMC/OQAM system.

References

[1] J.-S. Kim *et al.*, "OFDM versus filter bank multicarrier," *IEEE Signal Process. Mag.*, vol. 42, no. 4, pp. 92–112, 2011.
[2] L. Zhang, B. Liu, and X. Xin, "Secure optical generalized filter bank multi-carrier system based on cubic constellation masked method," *Opt. Lett.*, vol. 40, no. 12, pp. 2711–2714, 2015.
[3] H. Bouhadda, H. Shaiek, D. Roviras, R. Zayani, Y. Medjahdi, and R. Bouallegue, "Theoretical analysis of BER performance of nonlinearly amplified FBMC/OQAM and OFDM signals," *EURASIP J. Adv. Signal Process.*, vol. 2014, no. 1, pp. 1–16, 2014.
[4] G. Wunder *et al.*, "5GNOW: Challenging the LTE design paradigms of orthogonality and synchronicity," in *Proc. IEEE Veh. Technol. Conf.*, 2013, pp. 1–5, doi: 10.1109/VTCSpring.2013.6691814.
[5] D. Chen, D. Qu, T. Jiang, and Y. He, "Prototype filter optimization to minimize stopband energy with NPR constraint for filter bank multicarrier modulation systems," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 159–169, Jan. 2013.
[6] A. Saljoghei, F. A. Gutierrez, P. Perry, D. Venkitesh, R. D. Koipillai, and L. P. Barry, "Experimental comparison of FBMC and OFDM for multiple access uplink PON," *J. Light. Technol.*, vol. 35, no. 9, pp. 1595–1604, May 2017.
[7] D. Qu, F. Wang, Y. Wang, T. Jiang, and B. Farhang-Boroujeny, "Improving spectral efficiency of FBMC-OQAM through virtual symbols," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4204–4215, Jul. 2017.
[8] L. Li, Y. Wang, and L. Ding, "On the bit error probability of OFDM and FBMC-OQAM systems in Rayleigh and Rician multipath fading channels," *IEICE Trans. Commun.*, vol. E102B, no. 12, pp. 2276–2285, 2019.
[9] J. Zhao, S. Ni, and Y. Gong, "Peak-to-average power ratio reduction of FBMC/OQAM signal using a joint optimization scheme," *IEEE Access*, vol. 5, pp. 15810–15819, 2017, doi: 10.1109/ACCESS.2017.2700078.
[10] H. Wang, X. Wang, L. Xu, and W. Du, "Hybrid PAPR reduction scheme for FBMC/OQAM systems based on multi data block PTS and TR methods," *IEEE Access*, vol. 4, pp. 4761–4768, 2016, doi: 10.1109/ACCESS.2016.2605008.
[11] M. K. Srivastava, M. K. Shukla, N. Srivastava, and A. K. Shankhwar, "A hybrid scheme for low PAPR in filter bank multi carrier modulation," *Wireless Pers. Commun.*, vol. 113, no. 2, pp. 1009–1028, 2020.
[12] X. Yang, X. Hu, Z. Shen, H. He, W. Hu, and C. Bai, "Chaotic signal scrambling for physical layer security in OFDM-PON," in *Proc. Int. Conf. Transparent Opt. Netw.*, vol. 1, 2015, pp. 1–4.
[13] X. Yang, Z. Shen, X. Hu, and W. Hu, "Physical layer encryption algorithm for chaotic optical OFDM transmission against chosen-plaintext attacks," in *Proc. Int. Conf. Transparent Opt. Netw.*, 2016, pp. 1–5.
[14] Z. Zhao *et al.*, "Semiconductor-laser-based hybrid chaos source and its application in secure key distribution," *Opt. Lett.*, vol. 44, no. 10, pp. 2605–2608, 2019.
[15] T. Kodama *et al.*, "Secure 2.5 Gbit/s, 16-Ary OCDM block-ciphering with XOR using a single multi-port en/decoder," *J. Lightw. Technol.*, vol. 28, no. 1, pp. 181–187, 2010.
[16] 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. Light. Technol.*, vol. 35, no. 9, pp. 1524–1530, May 2017.

[17] B. Liu, L. Zhang, X. Xin, and J. Yu, "Constellation-masked secure communication technique for OFDM-PON," *Opt. Exp.*, vol. 20, no. 22, pp. 25161–25168, 2012.
[18] 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.
[19] J. Zhao *et al.*, "High security OFDM-PON of physical layer based on 4D-hyperchaos and dimension coordination optimization," *Opt. Exp.*, vol. 28, no. 14, pp. 21236–21246, 2020.
[20] L. Zhang, X. Xin, B. Liu, and X. Yin, "Physical secure enhancement in optical OFDMA-PON based on two-dimentional scrambling," in *Proc. Eur. Conf. Opt. Commun.*, 2012, no. 1, pp. 1–3.
[21] W. Zhang, C. 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. 2014.
[22] M. Bi *et al.*, "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.
[23] Y. Wang, P. Lei, H. Yang, and H. Cao, "Security analysis on a color image encryption based on DNA encoding and chaos map," *Comput. Elect. Eng.*, vol. 46, pp. 433–446, 2015, doi: 10.1016/j.compeleceng.2015.03.011.
[24] C. Zhu, Z. Gan, Y. Lu, and X. Chai, "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme," *Multimed. Tools Appl.*, vol. 79, no. 11–12, pp. 7227–7258, 2020.
[25] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, 2019, doi: 10.1016/j.sigpro.2018.09.029.
[26] 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. Light. Technol.*, vol. 36, no. 9, pp. 1706–1712, 2018.
[27] M. Bellanger, "FBMC physical layer: A primer," *PHYDYAS*, January, pp. 1–31, 2010, [Online]. Available: http://www.ict-phydyas.org/teamspace/internal-folder/FBMC-Primer_06-2010.pdf
[28] C. Grebogi, E. Ott, and J. A. Yorke, "Are three-frequency quasiperiodic orbits to be expected in typical nonlinear dynamical systems?," *Phys. Rev. Lett.*, vol. 51, no. 5, pp. 339–342, 1983.