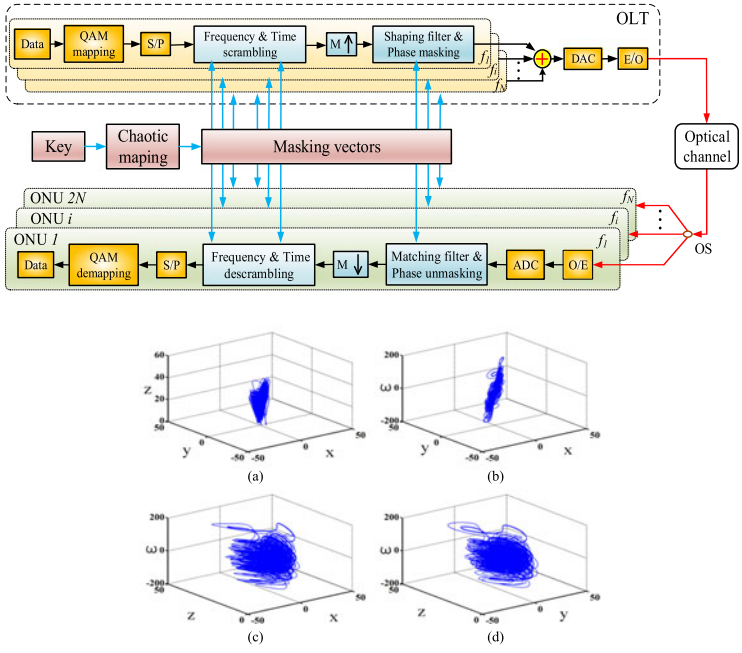
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Phase Masking and Time-Frequency Chaotic Encryption for DFMA-PON

Volume 10, Number 4, August 2018

Chongfu Zhang, *Senior Member, IEEE*
Yangyang Yan
Tingwei Wu
Xiaoling Zhang
Guangjun Wen
Kun Qiu



DOI: 10.1109/JPHOT.2018.2852299
1943-0655 © 2018 IEEE

Phase Masking and Time-Frequency Chaotic Encryption for DFMA-PON

Chongfu Zhang,[1,2] ***Senior Member, IEEE***, **Yangyang Yan**,[2] **Tingwei Wu**,[1,2] **Xiaoling Zhang**,[1,2] **Guangjun Wen**,[2] **and Kun Qiu**[2]

[1]School of Electronic and Information Engineering, University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China
[2]School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

DOI:10.1109/JPHOT.2018.2852299

Manuscript received May 9, 2018; revised June 26, 2018; accepted June 28, 2018. Date of publication June 2, 2018; date of current version June 12, 2018. This work was supported in part by the National Science Foundation of China under Grant 61571092 and in part by the Program for Joint Research of UESTC and Salton Tech No. 2018STKY001. Corresponding author: Chongfu Zhang (e-mail: cfzhang@uestc.edu.cn).

Abstract: We propose a novel physical layer security-enhanced digital filter multiple access-based passive optical network (DFMA-PON), for the first time to our best knowledge, by using phase masking and hybrid time-frequency domain chaotic scrambling. In the proposed secure DFMA-PON, all digital orthogonal filters have different random phase and the random phase is controlled by a hyperchaotic Chen system. The hyperchaotic Chen system is also adopted for the generation of scrambling matrices. In our demonstration, an encrypted signal has been experimentally transmitted over a 25-km standard single mode fiber in an intensity modulation/direct-detection DFMA-PON system. The experimental results verify that various attacks can be effectively prevented and indicate the proposed scheme as a promising solution for physical layer secure DFMA-PON systems.

Index Terms: Phase masking, physical layer, intensity modulation/direct-detection, digital filter multiple access.

1. Introduction

To enable access network not only adapting to highly dynamic traffic patterns but also offering on-demand connections/services, next generation access networks need to adopt much more advanced access technology [1]. Several access technologies have been reported, such as time division multiple access (TDMA), wavelength division multiple access (WDMA), hybrid TDMA/WDMA, frequency division multiple access (FDMA), and orthogonal frequency division multiple access (OFDMA). To meet the demand, all above access technologies need to be improved in reconfigurability, flexibility and elasticity. Digital filter multiple access (DFMA) [2] has been viewed as a promising candidate for future passive optical networks (PONs), owing to its numerous advantages such as functionality, flexibility, upgradability and great backward compatibility with existing PONs. Moreover, DFMA does not require the generation of sinusoidal carriers, mixers, or optical I/Q modulators, so it is relatively cost-effective [2], [3]. And DFMA has good spectra utilization and high bandwidth resource allocation flexibility. Therefore, DFMA-PON reveals great potential in next generation access networks.

With the increased accessibility of broadcast-based access networks, security has become one of the most important issues. To improve the security of access networks, secure methods in both the upper layer and the physical layer have been developed [4]–[22]. Since the upper layer cannot protect the control data or heads, the upper layer secure methods may be vulnerable [4]–[6]. What's more, the key management is a core problem for upper layer based secure methods. Compared with the upper layer encryption, physical layer security has the advantage that it can provide transparent encryption for all data. For the physical layer security, various techniques have been proposed, such as chaos and deoxyribonucleic acid encoding [5], chaotic laser communication [7], [8], exclusive or gate (XOR) [9], [10], chaotic pseudorandom RF subcarriers [11], and chaotic constellation transformation [12]. However, the low stability and the key distribution speed are two main problems for the practical use of chaotic laser communication. Moreover, since the key space of XOR is not large enough, it can be easily deciphered via a force attack. Chaos-based physical security methods have been considered as a promising solution for access networks, and some chaos-based physical security schemes have been proposed, such as chaotic frequency scrambling [11], [13]–[15], chaotic constellation scrambling [16], [17], hybrid chaotic encryption [5]–[18], chaotic fractional Fourier transformation [19], Brownian motion encryption [20], chaotic nonlinear encryption, and key space enhanced chaotic encryption [21], [22]. In chaotic frequency scrambling, the key space of the system is restricted because the encryption is realized in frequency domain, which makes it vulnerable to brute-force attack. In chaotic constellation scrambling, it just rotates the constellation of QAM symbols. In Brownian motion encryption, it can realize both symbol substituting and symbol interleaving. In hybrid chaotic and nonlinear encryption and chaotic fractional Fourier transformation, the complexity is high. However, the current works have focused on the security enhancement schemes for OFDMA-PON using chaotic encryption. DFMA-PON has emerged as one of the most promising solution to meet the flexibility requirement of next generation access networks. But the security of DFMA-PON has been barely investigated. This paper is an extension of our previous work presented in [23], with in-depth descriptions of the phase sensibility of digital filter and the chaos systems.

In this paper, we propose and experimentally demonstrate a three-dimensional (3-D) chaotic scrambling method to enhance the physical layer security of DFMA-PON systems. Phase masking and hybrid time-frequency domain chaotic scrambling are then employed. In the proposed secure DFMA-PON, digital orthogonal filters have different random phase and the random phase is controlled by a hyper-chaotic Chen system with complex dynamic trajectory [24]. The data on both frequency and time domain are then scrambled through the generated scrambling matrices. Finally, an encrypted DFMA signal transmission over a 25-km standard single-mode fiber (SSMF) has experimentally demonstrated in an intensity modulation/direct detection (IM/DD) DFMA-PON.

2. Principle

The schematic diagram of the proposed secure method for DFMA-PON is shown in Fig. 1. The original data are firstly mapped into QAM symbols, and then they are serial-to-parallel (S/P) converted. Subsequently, the parallel data undergo frequency and time scrambling, where the scrambling matrices are produced by the hyper-chaotic Chen system. The hyper-chaotic Chen system can be then given by,

$$\begin{cases} \dfrac{\partial \omega}{\partial t} = a(y - x) + \omega \\ \dfrac{\partial y}{\partial t} = dx - xz + cy \\ \dfrac{\partial z}{\partial t} = xy - bz \\ \dfrac{\partial \omega}{\partial t} = yz + r\omega \end{cases} \tag{1}$$

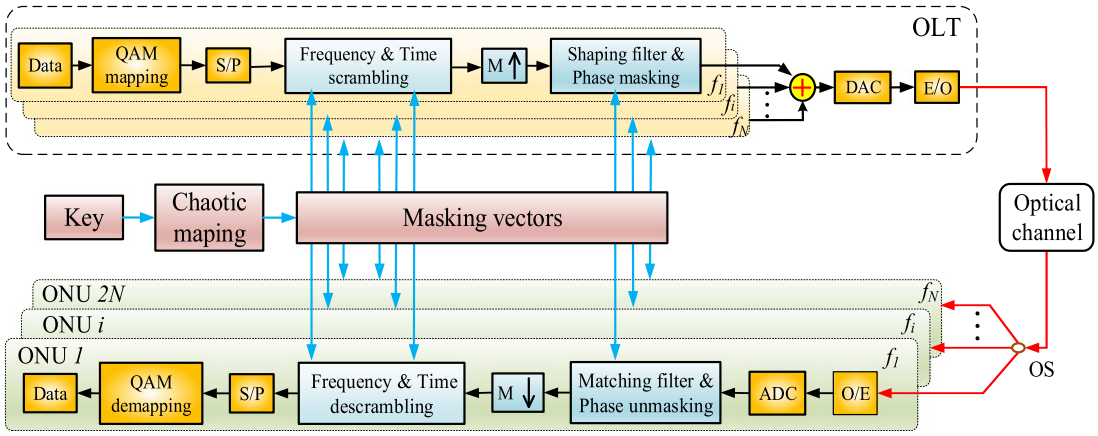


Fig. 1. Schematic diagram of proposed 3D chaos encryption in DFMA-PON.

where x, y, z, ω are the state variables and t is the time index. And a, b, c, d, r are the real constant parameters. When a = 35, b = 3, c = 12, d = 7, $0.085 < r \leq 0.798$, it is a hyper-chaotic system. x, y, z and ω are the outputs of this chaos system. This model can produce four chaotic sequences of (x, y, z, ω) simultaneously, which can be used to generate the scrambling matrices. In our scheme, x and (y, z, ω) are used for the generation of frequency and time scrambling matrices, respectively. In order to normalize the iteration values of Eq. (1), the decimal fractions of chaotic sequences (x, y, z, ω) can be represented by (x, y, z, ω) mod 1.

An OFDM frame is presented as a matrix PF $\times$ T, where F is the subcarrier number and T is the total OFDM symbol number. We define the frequency scrambling matrix as MF, the time scrambling matrix as MT, respectively. And the generation of MF and MT has been found in [25]. So the encrypted OFDM signal can be expressed as Ps = MF $\times$ PF $\times$ T $\times$ MT. After frequency and time scrambling, the data are up-sampled (M$\uparrow$) by a factor M via inserting M-1 zeros between two consecutive samples. After that, the up-sampled signal passes through a digital shaping filter and the phase of digital shaping filter is masked. All the digital orthogonal filters in the proposed secure DFMA-PON are constructed by using the Hilbert-pair approach [3]. The impulse responses of the ith Hilbert-pair hi(t) can be written as,

$$h_i^I(t) = p(t)\cos(2\pi f_{ci} + \phi_i) \tag{2a}$$

$$h_i^Q(t) = p(t)\sin(2\pi f_{ci} + \phi_i) \tag{2b}$$

where f_{ci} and φ_i are the central frequency and the phase of the ith Hilbert-pair, respectively. $p(t)$ is the baseband pulse, which is expressed by,

$$p(t) = \frac{\sin[\pi(1-\alpha)t'] + 4\alpha t'\cos[\pi(1+\alpha)t']}{\pi t'\left[1-(4\alpha t')^2\right]}, t' = t/T \tag{3}$$

and f_{ci} is given by,

$$f_{ci} = (2i-1)\frac{F_{sampling}}{2M}, i = 1, 2, 3\ldots \tag{4}$$

where $F_{sampling}$ is the sampling speed of digital to analog converter (DAC) and analog to digital converter (ADC).

The phase sequences (i.e., phase masking vectors) of all filters are produced by the hyper-chaotic Chen system. To enhance the security of the proposed secure DFMA-PON, the phase sequences are different for the filters with different frequencies, while the phase sequences are same for the filters with the same frequency. All the filters update their phases of every K data unit.

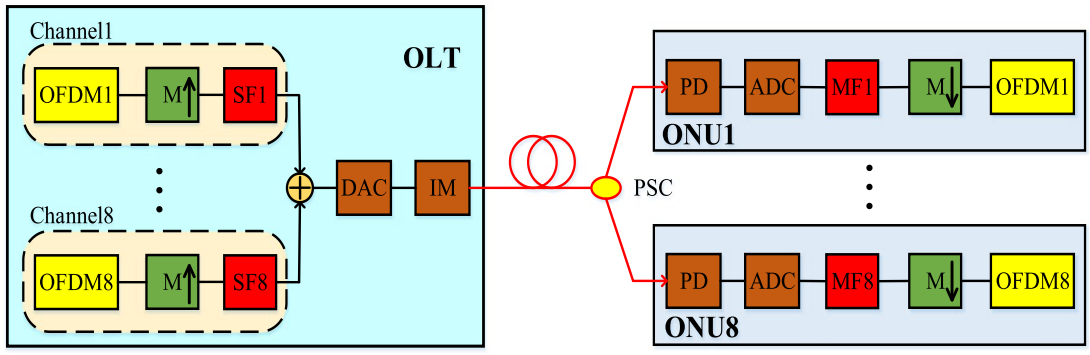


Fig. 2. Simulation setup of DFMA-PON.

The encrypted signals after optical channel are transmitted to different optical network units (ONU) through an optical splitter (OS).

At the ONU side, ONU can recover the signals by reverse processing. The impulse responses of matching filters are written as,

$$g_i^I(t) = h_i^I(-t)$$
$$g_i^Q(t) = h_i^Q(-t) \tag{5}$$

With the property,

$$g_i^A(t) \otimes h_j^B(t) = \begin{cases} \delta(t - t_0) & A = B \text{ and } i = j \\ 0 & A \neq B \text{ and } i \neq j \end{cases} \tag{6}$$

where the in-phase and the quadrature-phase filters of the Hilbert-pair are indicated by the superscripts "I" and "Q", respectively. t_0 is the time delay, which is induced by the digital filtering process.

3. Demonstration Setup, Results and Discussion

3.1 Phase Sensibility of Digital Filter in DFMA-PON

Simulation setup: The simulation setup of DFMA-PON is depicted in Fig. 2, where 8 OFDM channels are multiplexed and de-multiplexed using digital orthogonal filters. For each OFDM signal, it is firstly up-sampled by a factor of 8, and then passes through a digital shaping filter (SF). After filtering, all signals are coupled in the digital domain. Subsequently, they are fed into a DAC to perform digital to analogue conversion. Then the signals are modulated using an intensity modulator. After propagation along the SSMF, the optical signal reaches the ONU, where it passes through a photo detector (PD) and an ADC. Then, it is input into a matching filter (MF) to perform filtering. Subsequently, the signal is down-sampled by a factor of 8. After OFDM demodulation, the signal can be recovered. We perform the simulation by using MATLAB and VPI. To investigate the phase sensibility of digital filters, we fix the phases of all matching filters to 0 and change the phases of all shaping filters. The total 8 filters are used by 8 different ONUs. The $F_{sampling}$ is 10GSa/s and the phase-mismatch value is normalized to π.

Results and discussion: Fig. 3(a) and (b) show the bit error rate (BER) with the mismatch of phase values of 8 filters for back to back (B2B) and 25 km SSMF cases, respectively. The filter length L is 64 and the central frequency of the filter is given by Eq. (4), with $i = 1, 2, 3$ and 4. In both the cases, the corresponding results with the same filter show a similar performance. As the mismatch of phase values increases, the BER rises rapidly. When the mismatch of phase values is above 0.3 rad, the BER is above 10^{-1}. Compared with the in-phase filters (I-PF), the phase sensibility of the corresponding quadrature-phase filters (Q-PF) is improved of about 0.02 rad at a BER of

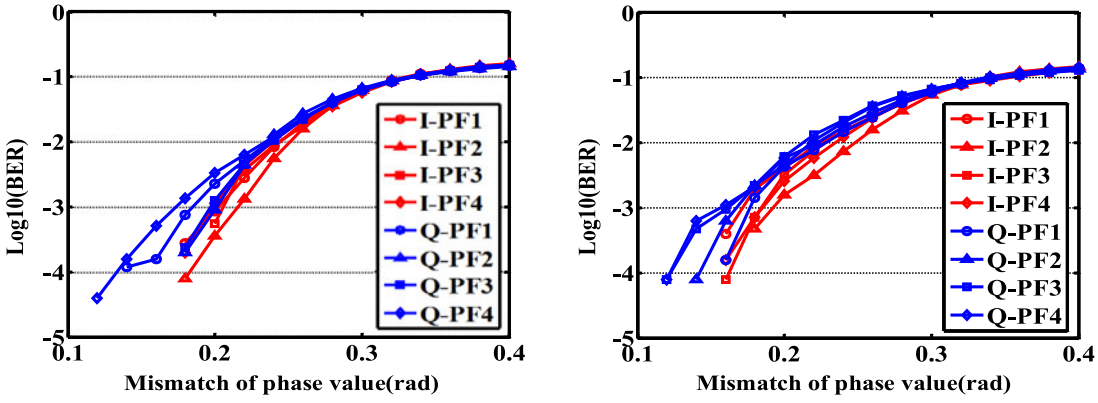


Fig. 3. BER with mismatch of phase values for BTB and 25 km SSMF in DFMA-PON.

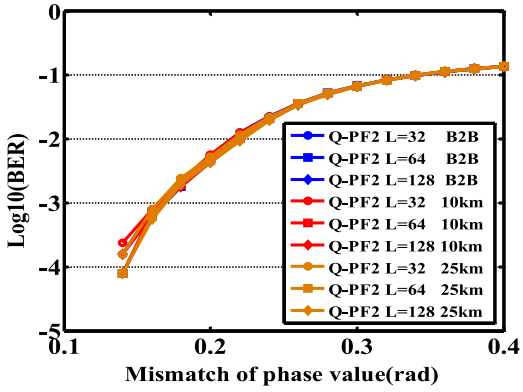


Fig. 4. BER with mismatch of phase values for different filter lengths *L* of 32, 64, and 128 in DFMA-PON.

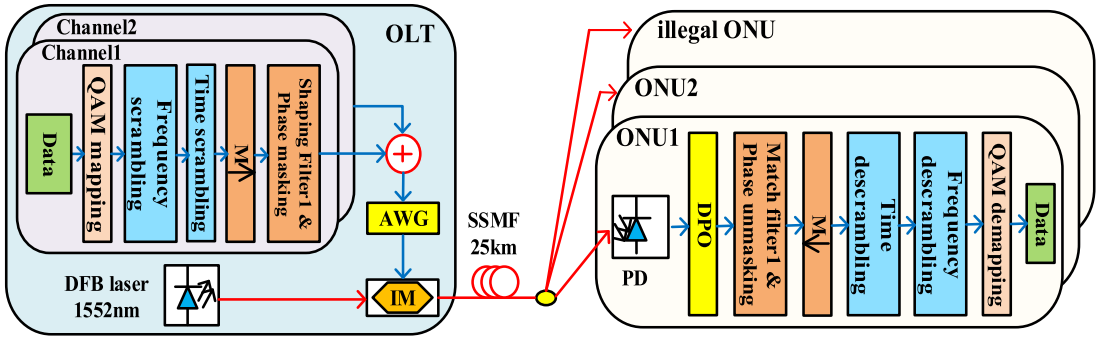


Fig. 5. Experimental setup for secure DFMA-PON based on 3D chaos encryption.

1×10^{-3}, which is mainly due to the fact that the I-PF has an intrinsic flat frequency response. Fig. 4 illustrates the BER with the mismatch of phase values to Q-PF2 for different L values under B2B, 10 and 25 km fibre transmission. These results indicate that the values of L have negligible influence to the phase sensibility.

3.2 Chaotic Characteristic and Measured Results

The experimental setup of the proposed secure DFMA-PON is shown in Fig. 5, where two regular ONUs with different matching filters are considered. The encrypted signal is generated by Matlab.

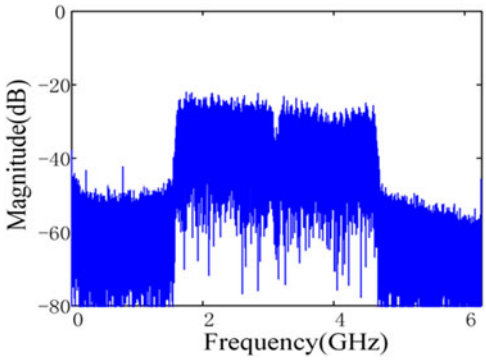


Fig. 6. Electrical spectra.

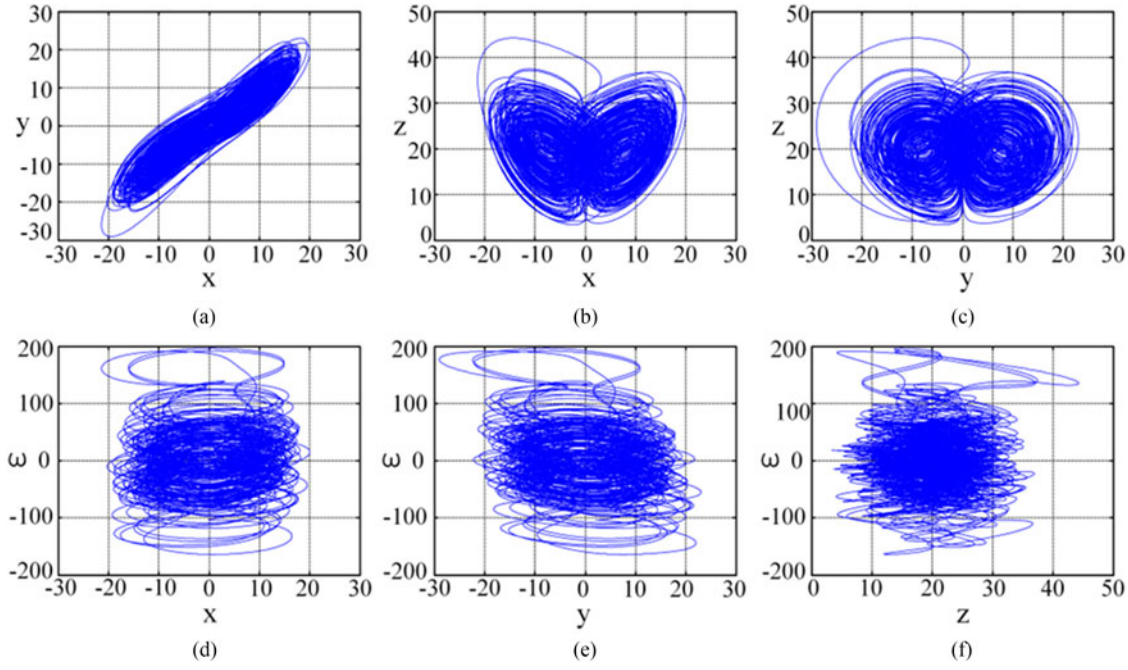


Fig. 7. 2-D phase diagrams of hyper-chaotic Chen system's chaotic model.

Firstly, two independent input data are mapped into 16-QAM sequences, which both have a length of 12000. After S/P conversion, there are two symbol matrixes with a size of 15×800. Then two symbol matrixes are scrambled by using the frequency and time scrambling matrices. After OFDM modulation, the number of subcarriers is 15, and 13 subcarriers are utilized to transmit valid data. The inverse FFT size is 32 and the cyclic prefix (CP) length is 1/8 of an OFDM symbol. The two OFDM channels are first up-sampled by a factor of 4 and pass through orthogonal shaping filters with a central frequency of 3.125 GHz. An arbitrary waveform generator (AWG) with a sample rate of 12.5 GSa/s is employed to generate the signal and the electrical spectra, as shown in Fig. 6. We can see that the bandwidth of the signal is about 3.125 GHz. A 1552-nm distributed feedback (DFB) laser is used as the light source. The modulated optical signal is directly sent into a 25-km SSMF-28 and the launched optical power is 2.6 dBm. After a PD, the received optical signal is directly detected and the sampling rate of the digital phosphor oscilloscope (DPO) is 25 GSa/s.

Figs. 7 and 8 show the 2-D and 3-D phase diagrams of hyper-chaotic Chen system's chaotic model, respectively. When $a = 35$, $b = 3$, $c = 12$, $d = 7$, the phase diagrams are with $(x_0, y_0, z_0, \omega_0, r) = (-4, -3, 5, -6, 0.58)$ and they exhibit complex dynamics of bifurcation and

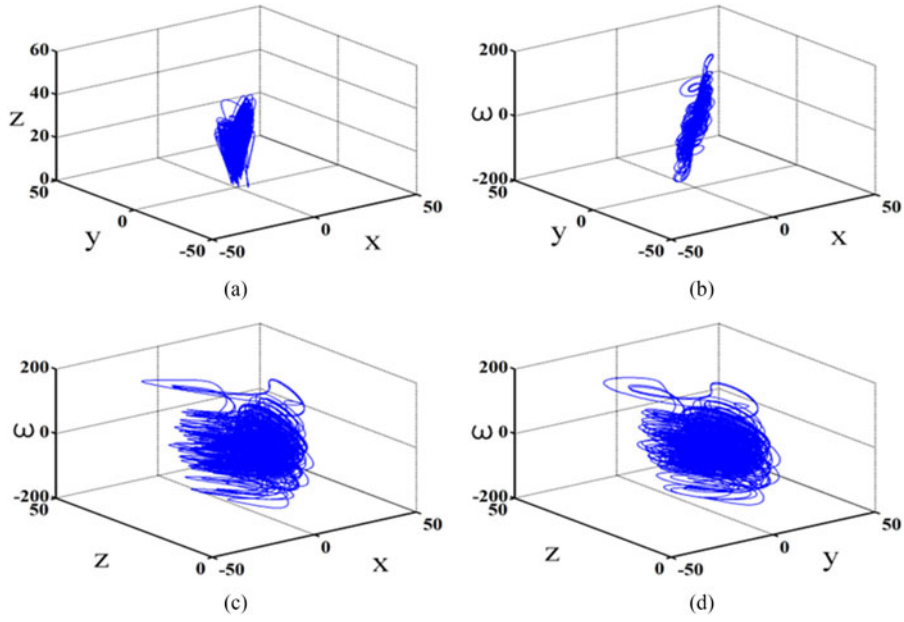


Fig. 8. 3-D phase diagrams of hyper-chaotic Chen system's chaotic model.

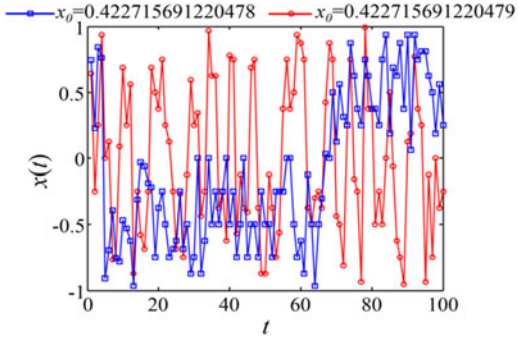


Fig 9. Sensibility of hyper-chaotic Chen system to change of the initial value x_0.

chaos, which indicates a good characteristic for encryption and makes it difficult to reconstruct the phase for illegal user. The sensibility of hyper-chaotic Chen system to change of the initial value x_0 is shown in Fig. 9. Here, we simulate 100 iteration times with the initial value of 1×10^{-15}. It can be seen that even two keys with tiny difference while two cases with total different iteration orbits, which indicates the chaotic sequence with good unpredictability. The statistical correlation curves of the generated encryption sequence are illustrated in Fig. 10. The number of iteration times is 1000 and the results indicate that the generated encryption sequences have good random characteristic.

In the proposed solution, a 3-D chaotic scrambling method is employed to enhance the physical layer security of DFMA-PON systems. The original data are performed in time and frequency scrambling firstly using scrambling matrices before IFFT, where the hyper-chaotic Chen system is used to generate the scrambling matrices. Because the hyper-chaotic Chen system has shown complex chaos and good randomness, so the scrambling effect of scrambling matrices can be ensured. When time and frequency scrambling is accomplished, the sequence of the original data is greatly scrambled. In addition, a random phase is employed by all digital orthogonal filters, where the random phase is controlled by a hyper-chaotic Chen system. During the filtering, the phase of all filters is changing so it can prevent illegal user get the information via match the phase of filter. Thus the proposed solution has good performance to enhance the security.

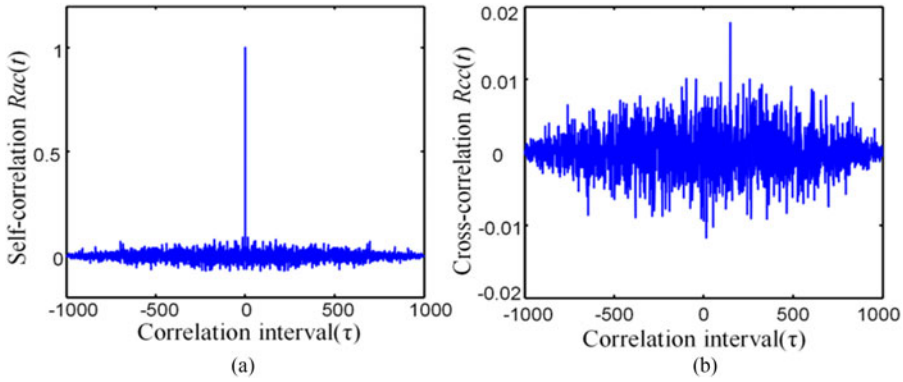


Fig. 10. Correlation of chaotic sequence, (a) auto-correlation for $x_0 = 1.256367428761492$; (b) cross-correlation for $x_0 = 1.256367428761492$ and $x_0 = 1.256367428761493$.

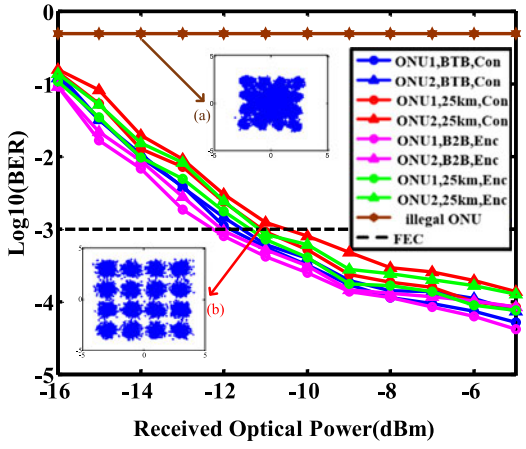


Fig. 11. BER curves for different ONUs, when $f_c = 3.125$ G/ Hz, M = 4, L = 64.

In the proposed solution, the security keys can be expressed as $\{x_0, y_0, z_0, \omega_0, r\}$, therefore the size of the key space is $(2^{31} \times 2^{31} \times 2^{31} \times 2^{31} \times 2^{31})^2 = 2.09 \times 10^{93}$ if a single-float value is adopted. Thus it can provide sufficient security against brute-force attacks. The complexity of the encrypted sequences mainly due to the generation of random number and scrambling matrix. Hypothesis the length of input data is N, so the computational complexity of the generation of the random number and the scrambling matrix is O(N) and O(N*$\log_2$(N)), respectively. So the complexity of the encrypted sequences is O(N*$\log_2$(N)). In the experiment, a personal computer (PC) with a 3.40 GHz Intel Core i7-6700 has been used. Then we found that all process time is 40.113 s and 42.544 s without/with the encryption process, respectively, indicating that the proposed encryption scheme has relatively low computational complexity.

Fig. 11 illustrates the measured BER for different ONUs with different cases. It can be observed that the received optical power of secure DFMA signal is 0.4 dB lower than that of conventional DFMA signal at a BER of 10^{-3} (FEC limit). Compared with ONU1, the receiver sensitivity of ONU2 at a BER of 10^{-3} is improved by 0.2 dB, which is mainly due to the fact that the filter of ONU1 has an intrinsic flat frequency response. For two regular ONUs, the power penalties are both about 0.3 dB at a BER of 1×10^{-3} before and after transmission. The BER of any illegal ONU is around 0.5, which indicates that an illegal ONU cannot obtain any useful information due to robust information encryption. The constellation diagrams at illegal ONU and legal ONUs are shown in inset (a) and inset (b) of Fig. 11, respectively, which have verified that the encrypted downstream DFMA signal cannot be correctly recovered by any illegal ONU.

4. Conclusion

We have proposed and experimentally demonstrated a phase masking and hybrid time-frequency chaotic scrambling scheme to realize the physical layer security for DFMA-PON. An encrypted signal has been successfully demonstrated in the experiment. The experimental results have verified that various attacks could be effectively prevented by the proposed encryption technique. Therefore, the proposed phase masking and hybrid time-frequency domain chaotic scrambling technique would be a promising solution to enhance the physical layer security of DFMA-PON.

References

[1] F. J. Effenberger, H. Mukai, S. Park S, and T. Pfeiffer, "Next-generation PON-part II: Candidate systems for next-generation PON," *IEEE Commun., Mag.*, vol. 47, no. 11, pp. 50–57, Nov. 2009.

[2] M. Bolea, R. P. Giddings, M. Bouich, C. Aupetit-Berthelemot, and J. M. Tang, "Digital filter multiple access PONs with DSP-enabled software reconfigurability," *J. Opt. Commun. Netw.*, vol. 7, no. 4, pp. 215–222, Apr. 2015.

[3] M. Bolea, R. P. Giddings, and J. M. Tang, "Digital orthogonal filter-enabled optical OFDM channel multiplexing for software-reconfigurable elastic PONs," *J. Lightw. Technol.*, vol. 32, no. 6, pp. 1200–1206, Jan. 2014.

[4] G. Wang, J. Chang, and P. R. Prucnal, "Theoretical analysis and experimental investigation on the security performance of incoherent optical CDMA code," *J. Lightw. Technol.*, vol. 28, no. 12, pp. 1761–1769, Jun. 2010.

[5] C. F. Zhang, W. Zhang, C. Chen, X. J. He, and K. Qiu, "Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding," *J. Lightw. Technol.*, vol. 36, no. 9, pp. 1706–1712, May 2018.

[6] M. C. Yuang *et al.*, "A high-performance OFDMA PON system architecture and medium access control," *J. Lightw. Technol.*, vol. 30, no. 11, pp. 1685–1693, Feb. 2012.

[7] G. D. VanWiggeren and R. Roy, "Communication with chaotic lasers," *Science*, vol. 279, no. 5354, pp. 1198–1200, Feb. 1998.

[8] N. Jiang, C. F. Zhang, and K. Qiu, "Secure passive optical network based on chaos synchronization," *Opt. Lett.*, vol. 37, no. 21, pp. 4501–4503, Nov. 2012.

[9] Z. X. Wang, Y. K. Huang, Y. H. Deng, J. Chang, and P. R. Prucnal, "Optical encryption with OCDMA code swapping using all-optical XOR logic gate," *IEEE Photon. Technol. Lett.*, vol. 21, no. 7, pp. 411–413, May 2009.

[10] M. P. Fok and P. R. Prucnal, "Polarization effect on optical XOR performance based on four-wave mixing," *IEEE Photon. Technol. Lett.*, vol. 22, no. 15, pp. 1096–1098, Aug. 2010.

[11] C. F. 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.

[12] W. Zhang, C. F. Zhang, C. Chen, and K. Qiu, "Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1524–1530, May 2017.

[13] L. J. Zhang, X. J. Xin, B. Liu, and Y. J. Wang, "Secure OFDM-PON based on chaos scrambling," *IEEE Photon. Technol. Lett.*, vol. 23, no. 14, pp. 998–1000, May 2011.

[14] L. J. Zhang, X. J. Xin, B. Liu, and J. J. Yu, "Physical-enhanced secure strategy in an OFDM-PON," *Opt. Exp.*, vol. 20, no. 3, pp. 2255–2265, Jan. 2012.

[15] B. Liu, X. Xin, L. Zhang, C. Yu, and Q. Zhang, "Physical-enhanced secure strategy in an OFDM-PON," in *Proc. Opt. Fiber Commun. Conf.*, Mar. 2012, paper OW3B–4.

[16] W. Zhang, C. F. Zhang, C. Chen, W. Jin, 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, Jul. 2014.

[17] W. Zhang, C. F. 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, Feb. 2016.

[18] M. F. Cheng *et al.*, "Enhanced secure strategy for OFDM-PON system by using hyper chaotic system and fractional Fourier transformation," *IEEE Photon. J.*, vol. 6, no. 6, Dec. 2014, Art. no. 7903409.

[19] L. Deng *et al.*, "Secure OFDM-PON system based on chaos and fractional Fourier transform techniques," *J. Lightw. Technol.*, vol. 32, no. 15, pp. 2629–2635, Aug. 2014.

[20] W. Zhang, C. F. Zhang, C. Chen, H. J. 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.

[21] M. H. 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. 4, pp. 2147–2150, Oct. 2017.

[22] M. H. 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. Y. Yan, C. F. Zhang, H. J. Zhang, and K. Qiu, "Security-enhanced DFMA-PON based on three-dimensional chaos encryption," in *Proc. Asia Commun. Photon. Conf.*, 2017, paper Su2A.38.

[24] V. Sundarapandian and R. Karthikeyan, "Anti-synchronization of hyperchaotic lorenz andhyperchaotic chen systems by adaptive control," *Int. J. Eng. Sci. Technol.*, vol. 3, no. 5, pp. 41–50, 2012.

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