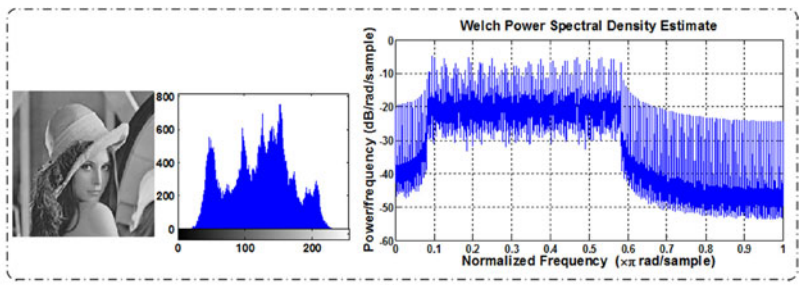
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

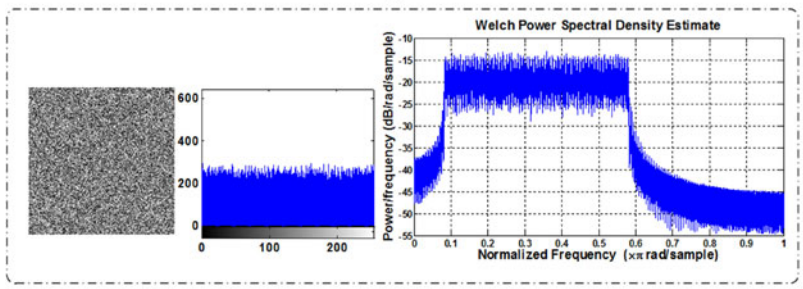
A Key Space Enhanced Chaotic Encryption Scheme for Physical Layer Security in OFDM-PON

Volume 9, Number 1, February 2017

Meihua Bi
Xiaosong Fu
Xuefang Zhou
Lu Zhang
Guowei Yang
XueLin Yang
Shilin Xiao
Weisheng Hu



(a)



(b)

DOI: 10.1109/JPHOT.2017.2661581
1943-0655 © 2017 IEEE

A Key Space Enhanced Chaotic Encryption Scheme for Physical Layer Security in OFDM-PON

Meihua Bi,[1,2] Xiaosong Fu,[1] Xuefang Zhou,[1] Lu Zhang,[2] Guowei Yang,[1] XueLin Yang,[2] Shilin Xiao,[2] and Weisheng Hu[2]

[1]College of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
[2]State Key Laboratory of Advanced Optical Communication System and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

DOI:10.1109/JPHOT.2017.2661581

Manuscript received December 7, 2016; revised January 14, 2017; accepted January 26, 2017. Date of publication February 7, 2017; date of current version February 21, 2017. This work was supported in part by the National Nature Science Fund of China under Grant 61501157, Grant 61431009, Grant 61571291, and Grant 61405051; in part by the Natural Science Foundation of Zhejiang Province under Grant LQ16F050004; and in part by the Scientific research project of Zhejiang Provincial Department of Education under Grant Y201533646. Corresponding author: M. Bi (e-mail: bmhua@hdu.edu.cn).

Abstract: In this paper, we propose a key space enhanced chaos-based encryption scheme with no requirement of redundant sideband information in an orthogonal frequency division multiplexing passive optical network (OFDM-PON). For the first time, a simple 1-D chaotic logistic map is employed to scramble the chaotic subcarrier allocation both in time/frequency domain and logical operation, which provides a huge key space to enhance the physical layer confidentiality. Due to the dynamic chaotic permutations, the largest key space is achieved in comparison with the reported encryption schemes in OFDM-PON. In addition, a ∼10-Gb/s secure transmission with encrypted OFDM data is experimentally demonstrated over 25-km standard single-mode fiber. The proposed encryption scheme demonstrates the excellent security of data transmission in OFDM-PON and the robustness against exhaustive attacks.

Index Terms: Orthogonal frequency-division multiplexing passive optical network (OFDM-PON), logistic map, key space enhanced, completed permutation.

1. Introduction

As the demand for broadband services increases rapidly, orthogonal frequency division multiplexing passive optical networks (OFDM-PON) have attracted massive attention in next generation optical access networks [1]. It endows the system with flexible resource allocation both in time and frequency domains, high spectral efficiency, and strong tolerance to fiber dispersion, and high data rate can be implemented with relatively low-bandwidth optical/electronic components [1]–[3]. However, in practical system, due to the broadcasting property of PON provided by the power splitter in optical distribution network, the system can easily suffer malicious eavesdropping or attacks from the illegal users, resulting in massive amounts of data being stolen, thereby posing a potentially serious threat to the user data where security is not considered [4], [5].

Currently, various schemes both in upper (such as media access control, MAC) and physical layer have been proposed to increase the security of PON [6]–[8]. Due to the unprotected information existing in MAC frame, the upper layer scheme may be vulnerable to the illegal users [9], [10]. While for the physical layer schemes, they can efficiently provide the overall protection for system, and make information impossibly be extracted by the malicious optical network units (ONUs) [11]. Among these proposed schemes in OFDM-PON, the chaos-based encryption method has been considered as the most promising solution due to its specific characteristics, such as the pseudo random, the ergodicity, *et al*. [12], [13]. By utilizing the nonlinearities of devices, the common optoelectronic devices-based chaotic system can produce the secret key to realize the security of system [14]. While, the extra optoelectronic devices with the same parameters' configurations are needed, which would increase the implementation difficulty and the cost of OFDM-PON. Therefore, the optoelectronic devices-based chaotic encryption method is not suitable for the OFDM-PON. To deal with this issue, the digital chaotic encryption is proposed. Owing to its easy implementation and integration with the digital signal processing (DSP) technique, the digital chaotic encryption has attracted more and more attention in the OFDM-PON [3], [6], [7]. Meanwhile, how to enlarge the key space of encryption is also considered as a crucial problem even in the chaos-based schemes. To achieve large key space, scaling the chaos mapping dimensional, time-frequency chaotic permutation, chaotic random mapping, and even combining the multi-dimension mapping and signal space permutation have been demonstrated [15]–[17], which would require redundant information or multiple iterations for transmitter and receiver, hence reducing the spectral efficiency and increasing the encryption complexity.

To deal with this problem, in this paper, we demonstrate a novel chaos-based physical layer security scheme with no any redundant information in OFDM-PON. By using the simple logical operation and full time/frequency permutations, the key space in this scheme is fully enlarged, and only simple 1-D chaos is employed to generate the partition information for XOR logical operation and the permutation weighted factor for realizing the multi-layer completed map. Owing to the combination of permutations and logistic operation, the proposed method has high sensitivity to the initial value of chaos so that only the legitimate ONUs with the correct keys can recover the correct chaotic sequences. Moreover, the feasibility of this scheme is successfully verified by experiment of 10-Gb/s 16-quadrature amplitude modulation (QAM) encrypted signals in OFDM-PON for 25-km standard single-mode fiber (SMF) transmission. The results show that, almost the same performance can be achieved between the system with and without the encryption scheme. In addition, compared to the previous researches [15], [18] with the same data matrix, our scheme provides a huge key space ($\sim 10^{287}$ for the case of 64 $\times$ 64 matrix), which further enhances the confidentiality of OFDM-PON.

2. Principles

The schematic diagram of the proposed encrypted scheme is plotted in Fig. 1, which is used among optical line terminal (OLT) and ONUs in OFDM-PON. At the transmitter, the pseudo-random binary sequence (PRBS) is injected into the logic model for realizing XOR operation with the chaotic sequence hence obtaining the first-fold encryption. Then, after the serial-to-parallel conversation (S/P), the encrypted data is mapped onto the QAM subcarriers, and is sent for multi-fold encryption permutations time/frequency domain.

To achieve the chaotic data, a simple 1-D logistic chaotic system is employed to generate the encryption information, which can reduce the complexity of chaotic generation, and this mapping is expressed as [19]

$$x_{n+1} = u x_n (1 - x_n)\ u \in (3.57, 4], x_n \in (0, 1) \tag{1}$$

where n presents the *n-th* iteration, and the u denotes the bifurcation parameter. As demonstrated in (1), x_n is the value of *n-th* iteration. It is proved that, when u within the range of (3.57, 4], this system presents good pseudo-random chaotic behavior with a certain initial iteration steps ($\sim$1000). To simplify, the output of (1) is denoted as $\{x_i\}$ and its value changes from 0 to 1. As for $\{x_i\}$, the chaotic

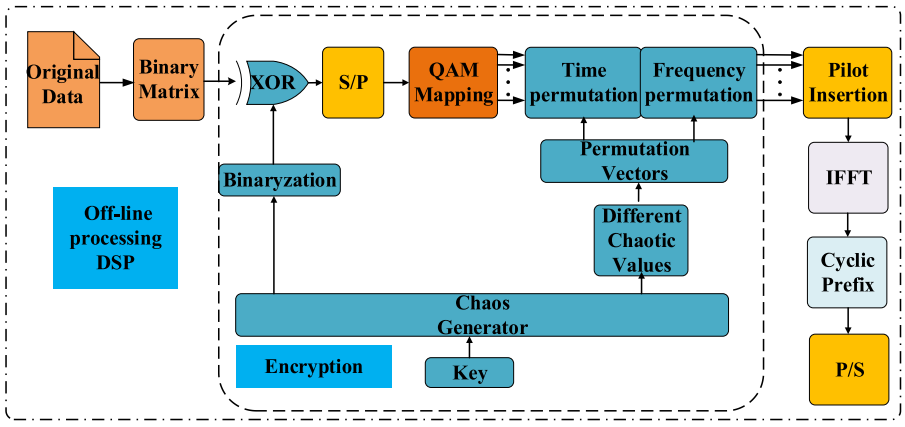


Fig. 1. Schematic diagram of the proposed encryption scheme at the transmitter.

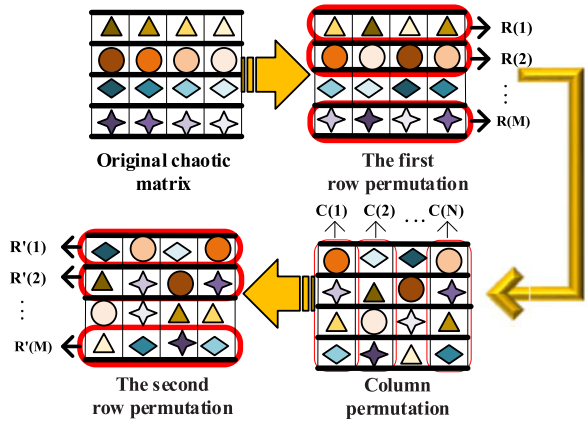


Fig. 2. Schematic diagram of the proposed chaotic permutation matrix to obtain permutation vectors.

orbit becomes entirely different when its initial value has a tiny discrepancy. These characteristics are suitable for secure transmission. In addition, to obtain digital chaotic sequences with the uniform distribution, the post-processing binaryzation is implemented, which is presented as

$$b_i = \begin{cases} 0, & x_i \le 0.5 \\ 1, & x_i > 0.5 \end{cases} (1 \le i \le n). \tag{2}$$

Passing through this processing, the integer 0 or 1 is obtained for the generation of chaotic sequence. For the first-fold encryption, the output of $\{b_i\}$ is applied to implement the XOR operation with original binary data, and this processing can be presented as

$$p_i' = p_i \oplus b_i \, (i = 1, 2...n) \tag{3}$$

where the symbol $\oplus$ is the XOR operator, p_i is the *i-th* original data. Based on (3), the first-fold encrypted data p_i' is obtained.

In addition, using the (1), chaotic sequences $\{x_k\}$ are generated in which different values are used to conduct the chaotic matrix thereby to create the complete encryption permutation. Here, the number of row and columns of this matrix is equal to OFDM signals. For instance, this matrix is set to M rows and N columns, and the chaotic permutation procedure is demonstrated in Fig. 2 which is composed by three steps as follows. The first step is to generate the row permutation vectors, the second is to perform column operation, and the third is to perform row permutation once

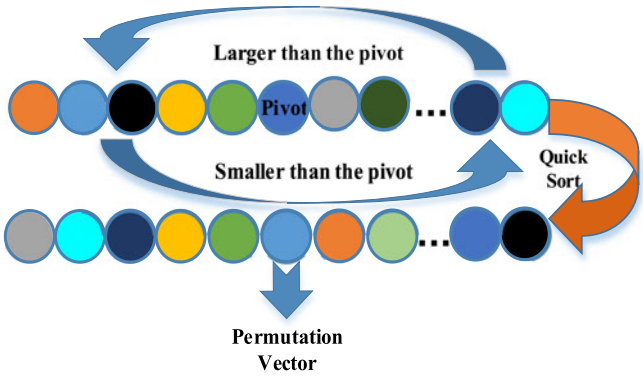


Fig. 3. Principle of quick sorting for acquiring permutation vector.

again. Throughout these steps, the position of chaotic data in original chaotic matrix is completely randomized. And, the permutation procedure is presented in details as follows. For the first row permutation processing, the chaos data in row are post-processed as

$$R(i) = Sort(X(i)) \quad i = 1, 2...M \tag{4}$$

where *X(i)* is the *i-th* row vector in matrix, which is corresponding to the $\{x_k\}$. The *Sort(X(i))* returns a dynamic row index of permutation vector, which is reset in a particular way with the index of *X(i)* and denoted as $R(i) = [r_1, r_2, \ldots, r_N]$. The specific sorting process for *Sort(X(i))* can be furthermore explained as in Fig. 3, which is based on quick sorting algorithm [20]. The basic idea following as: For each row, pick up an element as pivot, and then execute partition arrangement to realize that all elements smaller than the pivot would be moved to the front of pivot, while all elements bigger than the pivot would be moved to the behind of pivot. After the partition arrangement, the pivot is put in the final exchanged position. Eventually, the changed row index is taken as permutation vector. In this way, the permutation vector can be dynamically changed for each row.

Similarly, with almost the same processing, the second step with column permutation and the third step are implemented. The corresponding permutation index can be presented as $C(j) = [c_1, c_2, \ldots c_M]$ and $R'(i) = [r'_1, r'_2, \ldots, r'_N]$ respectively. After these three-times steps, we can achieve three chaotic permutation vectors which is used to reset the indexes of row and column of OFDM signals thereby realizing the completed encryption permutation. The original OFDM data matrix is given as

$$S_{M\times N}\begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1N} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ s_{M1} & s_{M2} & \cdots & s_{MN} \end{bmatrix} = \begin{bmatrix} \alpha(1) \\ \alpha(2) \\ \cdots \\ \cdots \\ \alpha(M) \end{bmatrix} \tag{5}$$

where the $s_{ij}\,(i = 1, 2 \ldots M,\ j = 1, 2, \ldots N)$ is the complex data after QAM mapped, and the row vector of the original OFDM signals is defined as *α(1),α(2),. . . α(M)*. Here, N and M are used to depict the number of OFDM symbols and subcarriers respectively. By using the permutation vectors *R(1),R(2),. . . R(M)*, the row (time) permutation is performed, and the OFDM frame matrix can be expressed as

$$S^r_{M\times N} = \begin{bmatrix} \alpha(R(1)) \\ \alpha(R(2)) \\ \cdots \\ \cdots \\ \alpha(R(M)) \end{bmatrix} = [\beta(1), \beta(2), ...\beta(N)]. \tag{6}$$

Within this process, for each row, the data of OFDM have been completed reset by *R(i)*. In the same manner, we can get the column permutation by using the permutation vector *C(j)*. Based on these operations, the OFDM signal frame becomes

$$S^{rc}_{M\times N} = [\beta(C(1)), \beta(C(2)), ...\beta(C(N))] = \begin{bmatrix} \alpha'(1) \\ \alpha'(2) \\ \cdots \\ \cdots \\ \alpha'(M) \end{bmatrix}. \tag{7}$$

Based on the row permutation vectors *R'(i)*, the last permutations encrypted OFDM frame can be demonstrated as

$$S^{rcr}_{M\times N} = \begin{bmatrix} \alpha'(R'(1)) \\ \alpha'(R(2)) \\ \cdots \\ \cdots \\ \alpha'(R'(M)) \end{bmatrix} = \begin{bmatrix} s'_{11} & s'_{12} & \cdots & s'_{1N} \\ s'_{21} & s'_{22} & \cdots & s'_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ s'_{M1} & s'_{M2} & \cdots & s'_{MN} \end{bmatrix}. \tag{8}$$

Then, by the pilot insertion, inverse fast Fourier transform (IFFT), cycle prefix insertion, and P/S process, encrypted OFDM signals are generated and modulated onto the optical carrier for distributing to each ONU. The permutation vectors with different random chaotic data generate another-fold security, and it has great pseudo random characteristics hence improving the security of system. Meanwhile, owing to the reversible property of this scheme, the original data can be decrypted at legal ONU.

Moreover, to further illustrate the enhanced encryption characteristic, we compare the permutation encryption among the chaotic subcarrier allocation partial scrambling in [15] with ours. For instance, a 6 $\times$ 6 data matrix is used for comparative analysis, as shown in Fig. 4. According to the reference [15], after the row and column permutation, the data matrix finally becomes the new matrix as presented at the Fig. 4(a). It is clear that, by permuting operation, the unbroken row and column information of data are still left as shown in the boxes of this figure, and the column index is preserved for each row and vice versa, which will reduce the security of system to some degree. While for our scheme, after permutation for three times, the index of data is decided by different permutation vectors independently, so that the data in each column and row can be completed permutated. The corresponding results are shown in Fig. 4(b). It is easily shown that, the indexes of data in permutation matrix are completely scrambled, and no any row and column index residual information exist, which will significantly enlarge the key space hence improving the system confidentiality.

3. Experimental Setup

Following the configurations of Fig. 5, we conduct the encrypted OFDM-PON experiment, in which two ONUs are used to emulate the illegal and legal users respectively. At the OLT, all the encrypted OFDM signals are generated offline by MATLAB programs. The IFFT points of the OFDM symbols is set to 256, of which 64 sub-carriers are used to load 16-QAM mapped data and another 64 complex conjugate data of 16-QAM are chosen to be mapped into other subcarriers. The system block pilots conforming to the sampling theorem is adopted to execute channel estimation. The CP is set to 1/8 of OFDM symbols' length, which is used to prevent inter-symbol interference. It is noted that, the intensity modulation direct detection (IMDD) style is chosen for this experiment. Here, the encrypted OFDM data are uploaded into the arbitrary waveform generator (AWG, Tektronix, 7122C) with 20-GSample/s sampling rate to generate the electrical OFDM signals. This generated signals are used to drive Mach-Zehnder modulator (MZM) to produce the $\sim$10-Gb/s optical OFDM signals. A continuous-wave (CW) laser at 1550 nm is used as the optical carrier. Through an Erbium Doped Fiber Amplifier (EDFA), the generated optical OFDM signals are boosted to 10 dBm and then sent

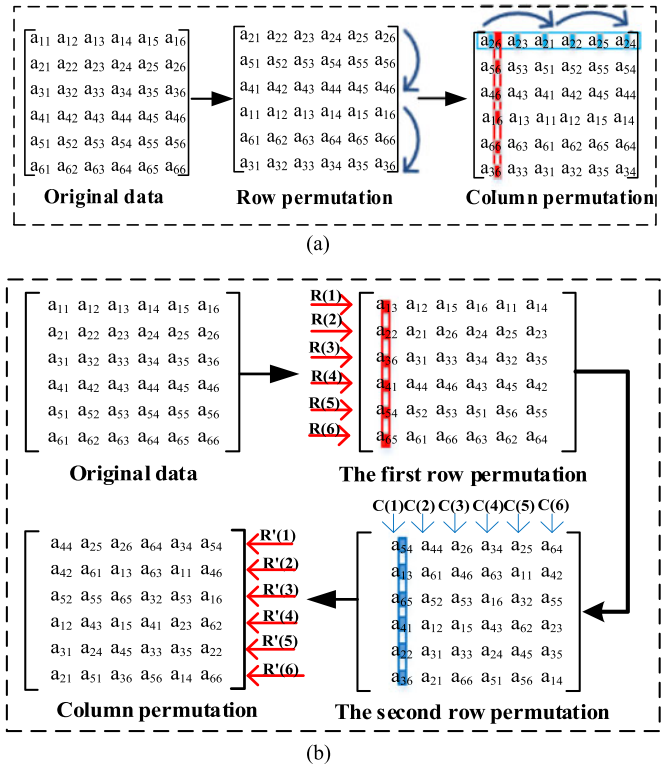


Fig. 4. Principle of (a) the partial permutation and (b) the completed permutation.

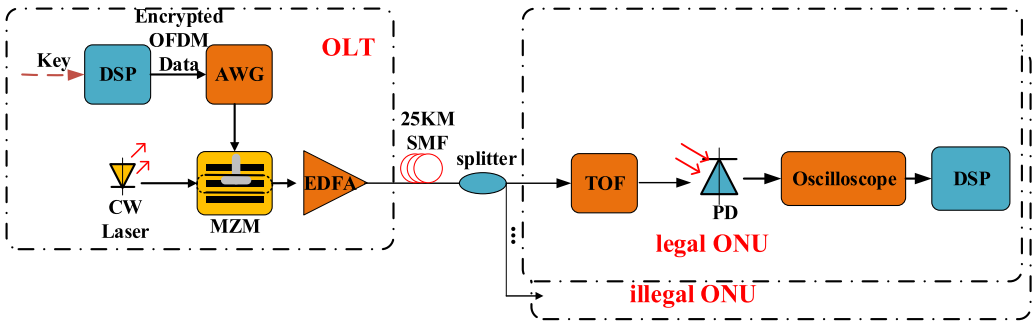


Fig. 5. Experimental setup for the secure transmission in OFDM-PON.

for transmission over a 25-km SMF. A variable optical attenuator installed in remote node is used to emulate the loss of optical power splitter.

After the SMF, the signals are distributed to each ONU through the power splitter. In each ONU, before the signal detection, a 100-GHz tunable optical filter (TOF) is applied to suppress the amplified spontaneous emission (ASE) noise. And, the OFDM electrical signals are recovered by a photoelectric detector (PD) and filtered by an electrical low-pass filter. At last, a real-time digital oscilloscope (LeCroy SDA 830Zi-A) with 40-GS/Sample is employed to realize signal sampling and digitalization. Then, the sampled electrical OFDM signals are uploaded into the Matlab program for offline processing, and the corresponding decryption and demodulation operations are implemented. Meanwhile, it is worth noting that, to reduce the effect of high peak-to-average power ratio (PAPR) of OFDM signals on our proposed encrypted system, the photoelectric devices with high linearity are used in experiment, such as the linear amplifier, the optical modulators (MZM), etc. In addition, an initial value of logistic map is served as the secret key, we set $x_0 = 0.61854656454$

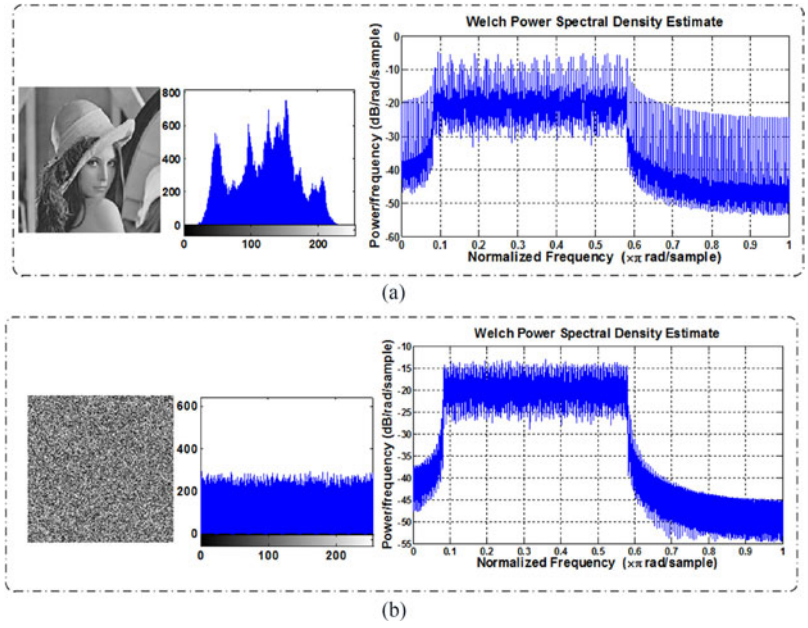


Fig. 6. Histograms and Welch's power spectral density. (a) Original and (b) encrypted data.

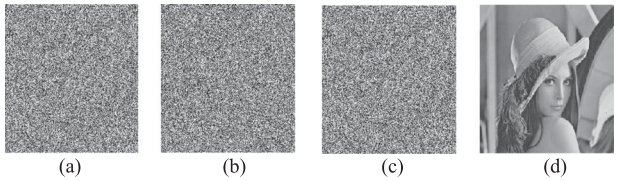


Fig. 7. Decryption in four different conditions. (a) Only correct key for XOR, (b) only correct key for permutation decryption, (c) wrong secure key for both XOR and permutation, and (d) correct decipher.

and $u = 3.9955454875$ (In generally, the u is set to near 4 to make sure that logistic sequence has a better pseudo randomness.), which is pre-shared at the legal ONUs and OLT in this experiment.

4. Results and Further Discussion

Firstly, to qualitatively evaluate our proposed scheme, classical image used in image processing system is encrypted for testing the secrecy of IMDD-based OFDM-PON. As shown in Fig. 6, we give the image, as well its histograms and Welch's power spectral density for the original encrypted image data. From Fig. 6(a), it is easily got that, due to the roughly histogram distribution feature of original data, the fluctuant power spectral density is obviously observed. And, in the middle of Fig. 6(a), the uneven lines in graph represent the irregular gray-level value information. While, for the encrypted case, we also present the image, histograms and power spectrum as depicted in Fig. 6(b). Compared to the original cases, no irregular image gray distribution and fluctuant power spectrum are observed.

Furthermore, to verify the high encrypted feature, we demonstrate the decrypted image information with different conditions for the illegal and legal ONUs as shown in Fig. 7. As for the illegal ONUs, no matter with the wrong key for XOR or permutation case, the original image data are not recovered and only the indistinguishable image is demonstrated as presented in Fig. 7(a)–(b). These results are similar with the complete wrong key cases for illegal ONUs in Fig. 7(c). While for the legal ONU, it is easily found that, the original image data can be completely recovered with almost no distortion, as depicted in Fig. 7(d). These features indicate that our proposed scheme have a high encryption in OFDM-PON.

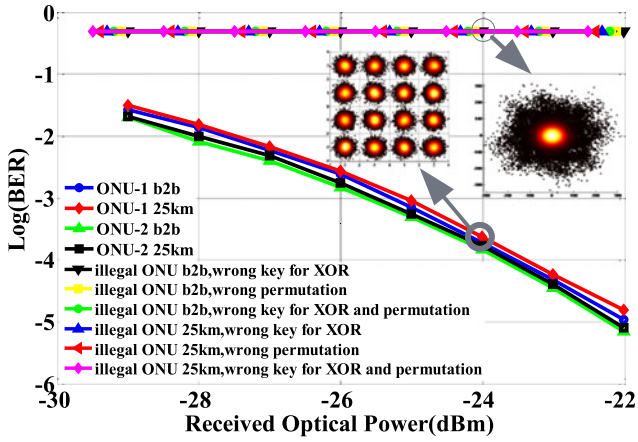


Fig. 8. BER measurements of the proposed encryption scheme for OFDM-PON.

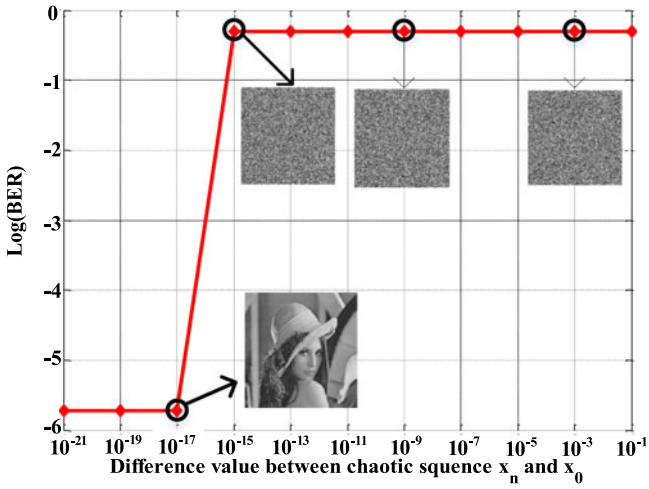


Fig. 9. BER curve versus difference between $\{x_n\}$ and x_0 at -21 dBm received optical power.

Moreover, we also measure the bit error ratio (BER) performance for two ONUs with back-to-back (BtB) and over 25-km SMF transmission in OFDM-PON. The corresponding results are plotted in Fig. 8. Since no BER difference for each ONU within the encrypted and non-encryption cases, we only select the sensitivity under the worst case to analyze. As for the legitimate ONUs, the original data can be correctly decrypted with only ~0.7-dB power penalty (BER@10^{-3}) for BtB and 25-km SMF transmission. In contrast, the BER increases to ~0.5 for any illegal ONU. It indicates that the original data can't be decrypted correctly even with a wrong key which has 10^{-15} discrepancy from the correct key. Apart from this, it is easily got that, no matter with the wrong key for XOR or permutation vector, the illegal users always achieve the bad BER of 0.5. Besides, the constellations diagrams for correct and wrong decrypted users are also plotted in Fig. 8, which further confirms our scheme a good resistance to the eavesdropping.

In addition, we also evaluate the tolerance of the initial values x_0 in this proposed OFDM-PON. Fig. 9 gives the BER curve @ ~ -21-dBm received optical power versus different values for the chaotic sequence $\{x_n\}$ with a tiny change of the initial values x_0. Here, the horizontal axis presents the difference value variation between the $\{x_n\}$ and x_0. It is easily got that, the encrypted data in our proposed system can be effectively recovered when the difference values are less than 10^{-15}. Namely, in the receiver end, only the wrong key has less than 10^{-15} discrepancy from the

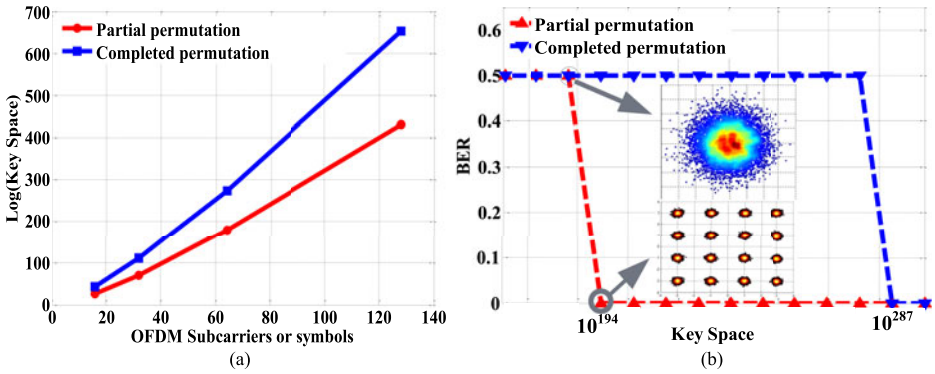


Fig. 10. (a) Measured key space curves with different OFDM subcarriers. (b) BER versus different key space.

TABLE I

COMPARISON OF ENCRYPTION METHODS AND CORRESPONDING KEY SPACE

Encryption scheme	Key space
Chaotic phase rotation + chaotic TS + Partial permutation in time-frequency domains matrix (M × N) with 4-D hyper Chaos map [15]	$(M = N = 64) \sim 10^{194}$
Multi-domain jointed dimension-transformed chaotic permutation in code, frequency and time domains(N × L) with 3-D Rossler chaotic model [17]	$(N = 256, L = 192) \sim 4.81 \times 10^{111}$
Chaotic PTS + chaotic TS with 4-D hyper chaos map [18]	$\sim 10^{120}$
Chaos scrambling in OFDM symbol, frequency and time domain with 1-D logistic map [21], [22]	$(M = N = 128)\, 3 \times 10^{215}$
Chaos scrambling in the OFDM frequency domain with 1-D logistic map [6]	$(M = N = 64) \sim 10^{90}$
Our scheme in this paper	$(M = N = 64) \sim 10^{287}$

correct key, the original data can be decrypted correctly. This can further guarantee the security of OFDM-PON.

Finally, we evaluate the key space of this proposed encryption scheme. Fig. 10(a) gives the size curve of key space with different OFDM subcarriers or symbols (here N equals to M). It is obviously observed that, compared to the scheme in [15], our scheme always achieves the higher key space, which can enhance the level of security to resist brutal force attack. Furthermore, to illustrate the important of key space, the BER performance with different key spaces for the scheme in [15] and ours is also measured, which is presented as in Fig. 10(b). Here, the chaos based logistic mapping creates a key space of 10^{15}. For sake of contrastive analysis, as in [15], the M and N of OFDM signals is also set to 64, to form the permutation matrix in both time and frequency domain, which can achieve a key space of $64! \times 64 \times 64! \times 64 \times 64! \times 64$ ($\sim 10^{272}$). In total, a huge key space of $\sim 10^{287}$ can be obtained. Assuming that the current fastest computing speed is $\sim 2.5 \times 10^{13}\, s^{-1}$ [18], $\sim 10^{266}$ years will be spent to obtain correct data via brutal-force attacks. From the Fig. 10(b), it is noted that, our scheme need the high space key for achieving no error BER feature in comparison with the scheme of [15], and the constellation diagrams with the 10^{194} key space for these two schemes are also demonstrated in this figure, which further verifies the effectiveness of our encryption scheme. In addition, we also give the key space comparison among different encryption methods with the cases of different dimensional chaotic maps and the same chaotic logistic maps as shown in Table I. It is obvious that, our proposed encrypted scheme always achieves the largest key space which would enhance the capacity of OFDM-PON to resist the brutal force attack.

5. Conclusion

We demonstrate a physical layer security improved scheme in OFDM-PON. For the first time, by the completed chaotic subcarrier allocation scrambling in both time and frequency domain and chaotic logical operation, the optical OFDM data can realize the encryption. In the encrypted process, the key space can achieve significantly enlarge, and it would increase with the increase of OFDM subcarriers (M) and symbols (N). As for the case of $N = M = 64$, a large key space of $\sim 10^{287}$ is created, which is verified that it is higher than current encryption schemes in OFDM-PON, leading to the increasing security for system. In this scheme, only simple 1-D logistic map is employed to generate the chaotic code and permutation matrix. Moreover, a ~10-Gb/s secure transmission with encrypted OFDM data is experimentally demonstrated over 25-km SMF, which verifies the feasibility of our scheme. A trail time of 10^{266} years and BER of 0.5 are obtained for the illegal ONUs with scrambling matrix of 64×64, which provides a promising solution of encryption transmission in future OFDM-PONs.

References

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

[2] M. Cvijetic, "Advanced technologies for next-generation fiber networks," in *Proc. Conf. Opt. Fiber Commun.*, 2010, vol. 45, pp. 1–3.

[3] L. Zhang, B. Liu, and X. Xin, "Secure coherent optical multi-carrier system with four-dimensional modulation space and Stokes vector scrambling," *Opt. Lett.*, vol. 40, no. 12, pp. 2858–2861, Jun. 2015.

[4] C. Guo, J. Liang, and R. Li, "Long-reach SSB-OFDM-PON employing fractional sampling and super-nyquist image induced aliasing," *J. Opt. Commun. Netw.*, vol. 7, no. 12, pp. 1120–1125, 2015.

[5] T. E. H. El-Gorashi, X. W. Dong, and J. M. H. Elmirghani, "Green optical orthogonal frequency-division multiplexing networks," *Optoelectron.*, vol. 8, no. 3, pp. 137–148, 2014.

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

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

[8] B. Liu, L. Zhang, X. Xin, and J. Yu, "Physical layer security in CO-OFDM transmission system using chaotic scrambling," *Opt. Commun.*, vol. 291, pp. 79–86, Mar 2013.

[9] M. Hossen, K.-D. Kim, and Y. Park, "Synchronized latency secured MAC protocol for PON based large sensor network," in *Proc. 12th Int. Conf. Adv. Commun. Technol.*, Feb. 2010, vol. 2, pp. 1528–1532.

[10] 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.

[11] C. Chen, C. Zhang, D. Liu, K. Qiu, and S. Liu, "Tunable optical frequency comb enabled scalable and cost-effective multiuser orthogonal frequency-division multiple access passive optical network with sourcefree optical network units," *Opt. Lett.*, vol. 37, no. 49, pp. 3954–3956, 2012.

[12] A. Argyris, E. Grivas, M. Hamacher, A. Bogris, and D. Syvridis, "Chaos-on-a-chip secures data transmission in optical fiber links," *Opt. Exp.*, vol. 18, no. 5, pp. 5188–5198, 2010.

[13] M. van Turnhout and F. Bociort, "Chaotic behavior in an algorithm to escape from poor local minima in lens design," *Opt. Exp.*, vol. 17, no. 8, pp. 6436–6450, 2009.

[14] A. Argyris, E. Grivas, A. Bogris, and D. Syvridis, "Transmission effects in wavelength division multiplexed chaotic optical communication systems," *J. Lightw. Technol.*, vol. 28, no. 21, pp. 3107–3114, Nov. 1, 2010.

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

[16] X. Hu, X. Yang, and W. Hu, "Chaos-based selected mapping scheme for physical layer security in OFDM-PON," *Electron. Lett.*, vol. 51, no. 18, pp. 1429–1431, Sep. 2015.

[17] B. Liu, L. Zhang, X. Xin, and Y. Wang, "Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation," *IEEE Photon. Technol. Lett.*, vol. 26, no. 2, pp. 127–130, Jan. 2014.

[18] 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.

[19] L. Liu, S. Miao, H. Hu, and Y. Deng, "Pseudorandom bit generator based on nonstationary logistic maps," *IET Inf. Security*, vol. 10, pp. 87–94, 2016.

[20] X. Wang, "Analysis of the time complexity of quick sort algorithm," in *Proc. 4th Int. Conf. Inf. Manage., Innovation Manage Ind. Eng.*, Nov. 2011, vol. 1, pp. 408–410.

[21] L. Zhang, X. Xin, B Liu, and X. Yin, "Physical secure enhancement in optical OFDMA-PON based on two-dimensional scrambling," in *Proc. ECOC*, Sep. 2012, pp. 1–3.

[22] L. Zhang, X. Xin, B. Liu, and X. Yin, "Physical secure enhancement in optical OFDMA-PON based on two-dimensional scrambling", *Opt. Exp.*, vol. 20, no. 26, pp. B32–B37, Dec. 10, 2012.