Physical-Layer Encryption Using Digital Chaos for Secure OFDM Transmission

Xuelin Yang, Adnan A.E. Hajomer and Weisheng Hu

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.68238

Abstract

Due to the broadcasting nature of passive optical network (PON), data security is challenging. For the transmission of orthogonal frequency division multiplexing (OFDM) signals, the high peak-to-average power ratio (PAPR) is considered as one of the major drawbacks. This chapter reviews the digital chaos-based secure OFDM data encryption schemes, where the transmission performance is improved via PAPR reduction. The digital chaos is incorporated into the signal scrambling approaches: selective mapping (SLM), partial transmit sequence (PTS); and precoding approaches: discrete Fourier transform (DFT) and Walsh-Hadamard transform (WHT) for PAPR reduction. Multi-fold data encryption is achieved with a huge key space provided by digital chaos, to enhance the physical-layer security for OFDM-PON, while the pseudo-random properties of digital chaos are applied for PAPR reduction, which consequently improves the transmission performance. The evidences of these encryption approaches are presented in terms of theories, simulations, as well as experimental demonstrations. The chaotic data encryption schemes could be promising candidates for next-generation OFDM-PON.

Keywords: orthogonal frequency division multiplexing (OFDM), peak-to-average power ratio (PAPR), digital chaos, passive optical network (PON)

1. Introduction

Over the last decades, passive optical network (PON) has been playing a vital role in data traffic explosion driven by broadband services such as high-definition television (HDTV), cloud computing, 3D television, video on demand (VoD) [1, 2], and so on, because it offers several potential benefits such as high capacity, low cost, and energy efficiency. In fact, PON is a broadcasting structure that extends for ~20–100 km from optical line terminal (OLT) to optical network units (ONUs), in which no active component (such as Erbium-doped fiber amplifier, EDFA) is employed. The broadcasting nature in the downstream data traffic and the huge number of subscribers in PON make the data more susceptible to be eavesdropped or attacked by illegal ONUs. For instance, during the ranging process, the OLT has to broadcast the serial number and ID information of the ranged ONUs; a malicious user could make use of this information for spoofing.

Comparing with the encryption in higher layers, for instance, media access control (MAC) layer, physical-layer encryption can protect the data as well as the control and header information. If the physical-layer data encryption is implemented, this type of spoofing can be avoided since the header and ID information are all encrypted within the physical-layer; thus, it becomes desirable for security enhancement in PON. For security reasons, churning procedure of scrambling the data for downstream connection has been defined in ITU-T G.983.1 standard (Section 8.3.5.6 [3]), which is based on a key sent from ONU to OLT through a secure channel with a defined protocol; however, the key is vulnerable to be broken due to its limited short key length.

Chaos communication has been proposed to provide a huge key space for data security enhancement attributed to its unpredictable nature of randomness, noise-like nature, and broadband. However, the implementation of chaotic optical communication (i.e., fast changing of chaotic optical carriers) requires identical devices with identical parameters for transmitter and receiver, which is quite restricted from real implementation. On the other hand, digital chaos has attracted notable attention recently as a flexible alternative to avoid the implementation difficulty for device-based optical chaos [4–10]. Because it offers very appealing properties from the perspective of data encryption such as ergodicity, pseudo-randomness, and high sensitivity to the initial values, digital chaos provides a huge key space for security applications. Moreover, due to flexible digital signal processing (DSP) in electric domain, digital chaos is easier to be applied.

Optical orthogonal frequency division multiplexing (OFDM) is regarded as a promising modulation technique for next-generation PON, owing to the advantages in high spectrum efficiency, cost-effectiveness, and tolerance to fiber dispersion. High-speed data rate of OFDM signals is achieved by parallel transmission of partially overlapped spectra, lower rate frequency domain tributaries [11]. Moreover, the generation, modulation, and demodulation of OFDM signals have to be performed using DSP in electric domain, therefore it provides a natural physical-layer environment, where digital chaos can be incorporated into OFDM data encryption during transmission. However, OFDM modulation often leads to high peak-to-average power ratio (PAPR), which is one of the most detrimental factors in OFDM signal transmission, as it causes power saturation and nonlinear distortion at the optical receiver while degrading the transmission performance. The pseudo-random properties of digital chaos are helpful for PAPR reduction of OFDM signals, which consequently improves the transmission performance.

In this chapter, OFDM data encryption schemes are reviewed in detail for physical-layer security enhancement based on digital chaos during transmission, while jointly the transmission performances are significantly improved because of the effective reduction in PAPR of OFDM signals. The rest of the chapter is organized as follows. In Section 2, the fundamental theory of PAPR reduction of OFDM signals is shown. The properties of digital chaos are presented in Section 3. In Section 4, the encryption schemes are illustrated in details. Conclusions are given in Section 5.

2. PAPR of OFDM signals

OFDM modulation is the superposition of many independent signals modulated onto individual subcarriers with equal-spaced bandwidth. **Figure 1** shows the overlapping of the subcarriers in frequency domain. High PAPR could be inevitable especially when a large number of subcarriers are in phase. As a result, the optical receiver with a wide linear range is required to accommodate a large dynamic range of PAPR [12].

If a block of N symbols is denoted as the vector X =[X_0, X_1, …, $X_{N\text{-}1}$] for OFDM signals, the vector X is oversampling by g (i.e., $g(N\text{-}1)$ zero-padding, ZP), where g is an integer greater than or equal one. Therefore, the complex envelop of OFDM signals is

$$x[n] = \frac{1}{\sqrt{N}} \sum_{i=0}^{Ng-1} X_i e^{\frac{2\pi in}{Ng}}, 0 \le n \le Ng - 1 \tag{1}$$

By definition, the PAPR of OFDM signals is

$$PAPR = 10 \log(\max(|x[n]|^2)/E(|x[n]|^2)) \tag{2}$$

From Eqs. (1) and (2), the oversampling factor must be greater than one for sufficient accuracy of PAPR calculation [13]. To evaluate the PAPR performance, the complementary cumulative distribution function (CCDF) is commonly simulated, which is defined as the PAPR probability exceeding a given threshold for a certain OFDM data block. Based on the central limit theorem, the real and imaginary parts of the complex OFDM signals after inverse fast Fourier transformation (IFFT) have Gaussian distribution in the case of sufficient large number of subcarriers, thus the amplitudes follow the Rayleigh distribution. For instance, if the CDF of the amplitude of a signal sample is given by

$$F(z) = 1 - e^{-z} \tag{3}$$

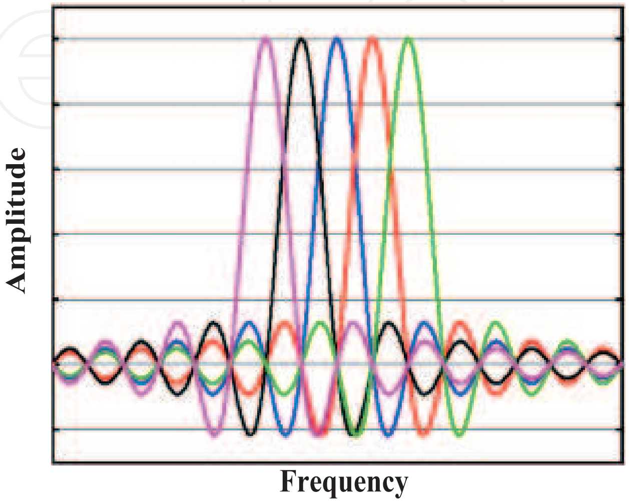


Figure 1. Spectrum of equal-spaced subcarriers in OFDM signals.

and N is a large number of samples, the CCDF of PAPR of the signal is [14]

$$P(PAPR > z) = 1 - P(PAPR \leq z) = 1 - F(z)^N = 1 - (1 - e^{-z})^N \tag{4}$$

3. Characteristics of digital chaos

Digital chaos has recently attracted numerous applications in OFDM-PONs [4–9], especially for data encryption, which is mainly due to the chaotic characteristics including pseudo-randomness, ergodicity, and high sensitivity to the initial values. Secure optical OFDM transmission is achieved by digital chaos, in which a huge key space is generated and predetermined by chaotic equations. Since the initial values and the other control parameters are utilized as the secure keys between OLT and ONUs, it provides a huge key space, which guarantees the physical-layer confidentiality. At ONUs, the same chaotic sequences are generated using the same keys for data recovering after reception.

The fundamental properties of digital chaos can be described, for example, via a 4-dimensional (4D) hyper chaos [15]

$$\begin{cases} \dot{x} = a(-x + y) + yzu \\ \dot{y} = b(x + y) - xzu \\ \dot{z} = cy - u + dxyu \\ \dot{u} = -eu + xyz \end{cases} \tag{5}$$

where a, b, c, d, and e are constant parameters. When $a = 35$, $b = 10$, $c = 80$, $d = 0.5$, and $e = 10$, these appropriate initial values bring the system into chaotic zones. Eq. (5) can be solved by Runge-Kutta method with a time step of $h = 0.001$. The solutions of Eq. (5) output the attractor diagrams of the 4D chaos, as plotted in **Figure 2**, where excellent chaotic behaviors in terms of pseudo-randomness and phase dynamics are illustrated.

In digital chaos, the chaotic state is very sensitive with respect to the initial values, thus even a tiny change or modification of the original initial values will let it enter into another different chaotic state. In **Figure 3(a)**, the variation curve is illustrated for the digital chaotic sequence $\{y_i\}$, under a slight change (1×10^{-15}) in the initial value of y_0. The auto- and cross-correlation functions $R_{ac}(\tau)$ and $R_{cc}(\tau)$ are plotted in **Figure 3(b) and (c)** respectively, which reveal the high sensitivity associated with the chaotic initial values, where τ is the time lag. The good quality of randomness observed in **Figure 3** is essential to guarantee high-level security reliability for data encryption.

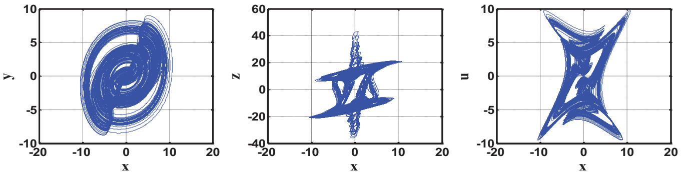


Figure 2. Chaotic attractor diagrams in phase planes of (x, y), (x, z), and (x, u).

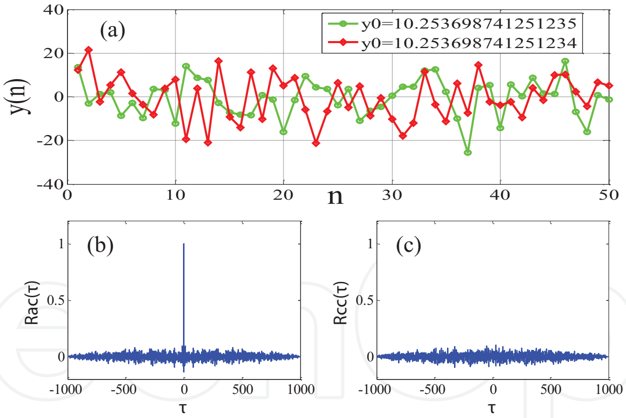


Figure 3. (a) Chaotic sequence of $\{y_i\}$ under tiny change of the initial values; (b) autocorrelation for y_0 =1.428121243912452; (c) cross-correlation for y_0 =1.428121243912452 and y_0 =1.428121243912453.

For a conservative estimate, a tiny change (~1×10^{-15}) of the initial values leads to a totally different chaotic state, as shown in **Figure 3**, therefore, the key space of 4D digital hyper chaos is ~10^{60} ($10^{15}\times10^{15}\times10^{15}\times10^{15}$).

Furthermore, the iteration times of chaotic differential equations and even the equations themselves can be served as the additional secure keys as well, so the actual key space will be >>10^{60}. Currently, the fastest computing speed is about $2.5\times10^{13}\text{s}^{-1}$, thus it will take ~$1.3\times10^{39}$ years to work out the possible initial keys of the 4D chaos via brutal-force trials [16]. Consequently, the chaotic data encryption provides a huge key space, which is large enough to resist exhaustive attacks.

4. Chaotic OFDM encryption with PAPR reduction

A variety of chaotic encryption schemes has been proposed for the physical-layer security in OFDM-PON [4–9], in which digital chaos has been incorporated into OFDM signal generation or modulation to enhance data security during transmission. However, in the existing chaotic secure schemes, the encryption is generally achieved without considering the improvement of transmission performance through the effective PAPR reduction in OFDM signals.

This section presents some systematic novel approaches to enhance the physical-layer security and jointly improve the OFDM transmission performances. The key idea behind these schemes is the combination of chaos-based encryption along with PAPR reduction; these approaches mainly belong to two categories of PAPR reduction: signal scrambling and matrix precoding, such as

- Chaotic signal scrambling: Chaotic partial transmit sequence (PTS) and chaotic selective mapping (SLM).
- Chaotic precoding: Discrete Fourier transform (DFT) and Walsh-Hadamard transform (WHT).

4.1. Chaotic signal scrambling

Signal scrambling is one of the traditional approaches in PAPR reduction. Chaotic sequences can be employed to scramble an input data block of OFDM symbols randomly, and then one of the scrambled OFDM signals with minimum PAPR is selected for final transmission. With the use of chaotic sequences in OFDM symbol scrambling, the physical-layer security is enhanced since the initial keys are required for correct recovery of the original OFDM data via correct counter-scrambling. At the same time, the transmission performance is improved simultaneously, owing to the effective reduction in PAPR via signal scrambling.

4.1.1. Chaotic partial transmit sequence (PTS)

The block diagram of OFDM data encryption using chaotic PTS is plotted in **Figure 4** [17]. After serial-to-parallel (S/P) conversion, a pseudo-random binary sequence (PRBS) is mapped onto QAM subcarriers, and then is sent for data encryption, which is applied via the following threefold encryption: chaotic training sequence (TS) insertion, chaotic random partition generation, and chaotic phase weighing factors generation.

Figure 5(a)–(c) shows the different partition examples in PTS scheme. Compared with the adjacent and interleaved partitions, the random partition provides the weakest cross-correlation among the sub-blocks, which leads to the largest PAPR reduction after selecting the optimum phase weighing factors. The PAPR can be minimized after searching for the optimized OFDM symbols for chaotic (random) signal scrambling.

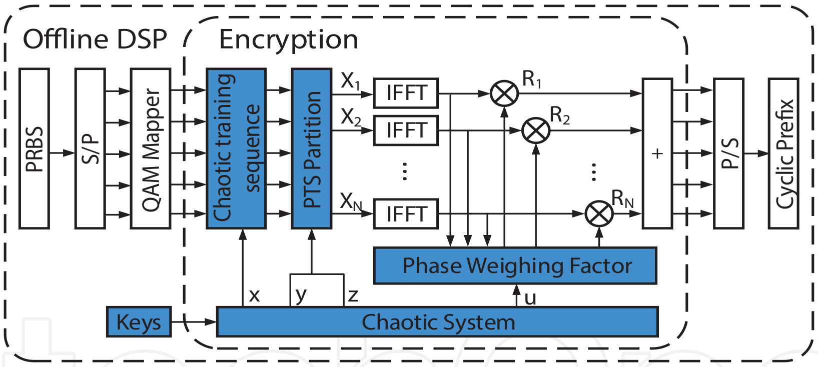


Figure 4. Schematic diagram of OFDM signal encryption using chaotic PTS.

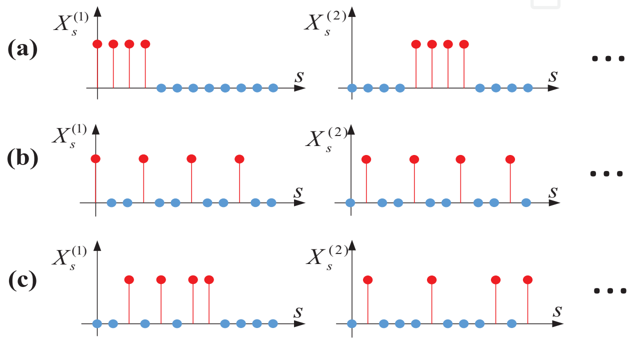


Figure 5. Partition design in PTS, for (a) adjacent; (b) interleaved; (c) random partitions.

To generate digitized chaotic sequences for OFDM signal encryption, the chaotic sequences obtained in Eq. (5) are processed using [18]

$$D_{x,i} = \mathrm{mod}(Extract(x_i, m, n, p), M) \tag{6}$$

where $Extract(x_i, m, n, p)$ outputs an integer, which is obtained by the mth, nth, and pth digits in the decimal part of x_i, mod(a, b) outputs the remainder of a divided by b, M is the maximum digital value in the digital sequence, which is 256 in all of our schemes [4]. Similarly, the other sequences $\{y_i\}$, $\{z_i\}$, and $\{u_i\}$ can be digitalized into $\{D_{y,i}\}$, $\{D_{z,i}\}$, and$\{D_{u,i}\}$. The details of chaotic PTS are given as follows.

The first sequence $\{D_{x,i}\}$ is applied to generate the chaotic TS for time synchronization of OFDM symbols. Since the illegal ONU does not have the information of chaotic TS, it has to try $(N_0+N)/N_0$ times on average to realize correct synchronization and demodulation, where N_0 is the length of cyclic prefix (CP). Moreover, due to the pseudo-random characteristic of digital chaos, it produces an autocorrelation similar to the δ function, which is advantageous for accurate OFDM symbol synchronization, as shown in **Figure 6(a)**. A legitimate ONU can correctly demodulate the original data; however, with a slight change in the initial keys, the peak does not appear, so that the data cannot be fully recovered, as illustrated in **Figure 6(b)**.

In chaotic (random) PTS, the chaotic sequences $\{D_{y,i}\}$, $\{D_{z,i}\}$, and $\{D_{u,i}\}$ can be employed to generate the partition information and the phase weighing factors. First, the digitized chaotic sequence $\{D_{y,i}\}$ is applied to generate the binary sequence $\{A_1\}$ using $\{\mathrm{mod}(D_{y,i},2)\}$. Similarly, the binary sequence can be generated by $\{D_{z,i}\}$. After bitwise logical operation of these two binary sequences, as shown in **Figure 7**, the chaotic random partition information $\{P^{(l)}\}$ is formed. The sub-blocks are then generated using $X^{(l)}= X\cdot P^{(l)}$, l =1, 2,···, L. where L denotes the total number of sub-blocks.

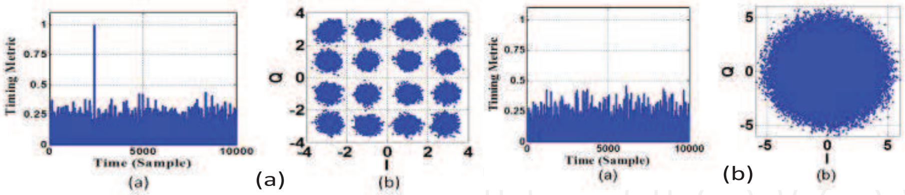
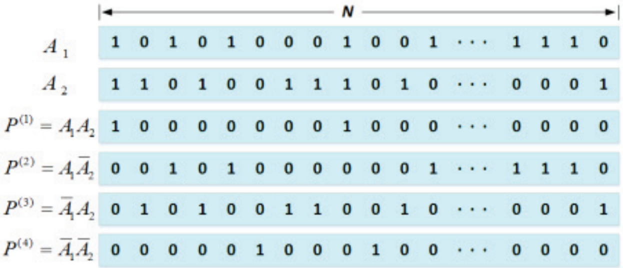


Figure 6. Effect of OFDM symbol time synchronization with (a) the right key; (b) a wrong key.



A_1	1	0	1	0	1	0	0	0	1	0	0	1	···	1	1	1	0
A_2	1	1	0	1	0	0	1	1	1	0	1	0	···	0	0	0	1
$P^{(1)} = A_1 A_2$	1	0	0	0	0	0	0	0	1	0	0	0	···	0	0	0	0
$P^{(2)} = A_1 \overline{A}_2$	0	0	1	0	1	0	0	0	0	0	0	1	···	1	1	1	0
$P^{(3)} = \overline{A}_1 A_2$	0	1	0	1	0	0	1	1	0	0	1	0	···	0	0	0	1
$P^{(4)} = \overline{A}_1 \overline{A}_2$	0	0	0	0	0	1	0	0	0	1	0	0	···	0	0	0	0

Figure 7. Generation of partition information (four sub-blocks) in chaotic PTS.

Second, the digitalized chaotic sequence $\{D_{u,i}\}$ is applied to generate the phase weighing factors R_l in PTS,

$$R_l = \exp\left(j \cdot 2\pi \cdot D_{u,\,i}/M\right) \quad (i = 1, 2, \ldots, K) \tag{7}$$

where K is the total number of phase weighing factors. After multiplying the phase weighing factors and transforming from frequency into time-domain, the corresponding time-domain vector becomes

$$x = \sum_{l=1}^{L} R_i x^{(l)} \tag{8}$$

$$x_n^{(l)} = \frac{1}{\sqrt{N}} \sum_{\mathrm{s}=0}^{N-1} X_s^{(l)} \exp\left(j\frac{2\pi sn}{N}\right) \tag{9}$$

where $x^{(l)}$ is the IFFT of $X^{(l)}$, s and n denote the indices of OFDM subcarrier and symbol, respectively.

In PTS, the combinations of sub-blocks and phase weighing factors are calculated to find the minimum PAPR, thus the final PAPR is

$$PAPR_{\mathrm{PTS}} = \min\Big(PAPR\Big(\sum_{l=1}^{L} R_i x^{(l)}\Big)\Big) \tag{10}$$

The final OFDM vector becomes

$$x_{pts} = \sum_{l=1}^{L} R_{l,\,\mathrm{opt}} x^{(l)} \tag{11}$$

where $R_{l,opt}$ is the optimized phase weighing factors. At ONUs, the decryption and demodulation procedures are the inverse operations that are implemented at OLT.

Since the initial values in digital chaos serve as the secure keys to recover the original OFDM signals, only legal ONUs can generate the same chaotic scrambling information with the correct secure keys that applied at OLT. By introducing digital chaos into signal scrambling, not only the security confidentiality of OFDM signal transmission is greatly enhanced, but also a performance-improved transmission can be expected with a lower PAPR.

As for the computational complexity, it is the same for the chaotic PTS and conventional random PTS. If compared with the case of OFDM transmission without PTS, the computational complexity of chaotic PTS scheme will be L^k times higher, which is inevitable for PAPR optimization. In our case, assuming four sub-blocks and two phase weighing factors, the computational complexity is 16 times higher for PAPR optimization; however, it guarantees both higher security and lower PAPR. Since the number of possible PTS partition states is 4^N ($4^{256} \approx 10^{154}$ in our case), it is hardly to be broken through brutal-force attacks. However, chaotic PTS still requires sideband information to transmit the partition and the phase factor information, which reduces the overall spectral efficiency in transmission.

4.1.2. Chaotic selected mapping (SLM)

As shown in **Figure 8**, chaotic SLM is another alternative data encryption scheme based on signal scrambling using digital chaotic sequences. In chaotic SLM, the digitized chaotic sequences can be obtained by processing of the chaotic sequences from 2D Henon chaos [19],

$$\begin{cases} x_{i+1} = 1 - \eta x_i^2 + y_i \\ y_{i+1} = \psi x_i \end{cases} \tag{12}$$

The input OFDM sequence is denoted as $X = [X_0, X_1, \ldots, X_{N-1}]$ in frequency domain, where X_k represents the complex data of the kth subcarrier, and N represents the total number of subcarriers. First, to implement the digital chaos into SLM scheme, the total number of the chaotic phase sequences is set to be V, and all of the phase sequences $P_v = [P_{v,0}, P_{v,1}, \ldots, P_{v,\ N-1}]$ $(1 \le v \le V)$ are obtained from the chaotic sequence $\{D_{y,i}\}$, where $P_{v,k} = exp(j \cdot 2\pi \cdot D_{y,k}/M), (0 \le k \le N-1)$. By component-wise vector multiplication of the input OFDM sequence X with the phase sequence $\{\mathrm{P}_v\}$, the input OFDM signals are encrypted fully via the chaotic sequences obtained in Eq. (12). The encrypted OFDM sequence $\{Y_v\}$ is

$$Y_v = X \otimes P_v = [X_0 P_{v,0}, X_1 P_{v,1}, \ \cdots, X_{N-1} P_{v,N-1}] \tag{13}$$

where ⊗ denotes the component-wise vector multiplication. Second, the IFFT is performed for all of the encrypted OFDM sequences $\{Y_v\}$

$$x_v = \mathrm{IFFT}(Y_v) \tag{14}$$

Finally, the OFDM signal sequence $\{x_v\}$ with minimum PAPR is chosen for OFDM transmission. It should be mentioned that in terms of computational complexity, better PAPR reduction can be expected with a larger V; however, the complexity will also increase due to the increased times of IFFT.

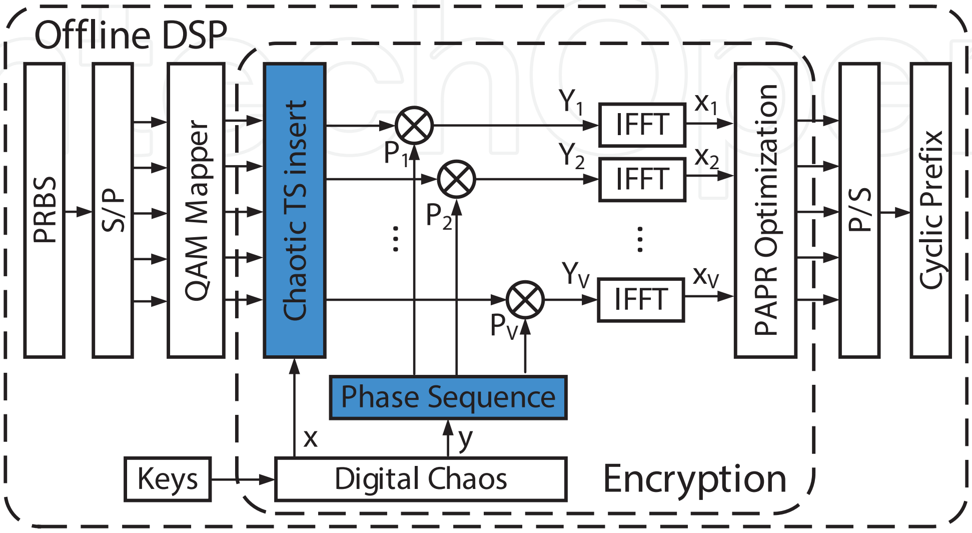


Figure 8. Schematic diagram of OFDM signal encryption using chaotic SLM.

4.1.3. Experiment results of chaotic PTS and SLM

The experimental setup of encrypted OFDM-PON transmission using chaotic PTS/SLM is shown in **Figure 9**. The input data stream was mapped onto 129 OFDM subcarriers at OLT, where 64 subcarriers were in the format of 16-QAM, and one subcarrier was unfilled with DC. The other 64 subcarriers had to be set as the complex conjugate of the aforementioned 64 subcarriers, where Hermitian symmetry had to be satisfied to realize intensity modulation and direct detection (IM/DD) after IFFT. After TS insertion for OFDM symbol time synchronization, chaotic PTS/SLM optimization and parallel-to-serial (P/S) conversion, a CP of 1/8 length of OFDM symbol was added into each OFDM symbol.

The above processing steps were performed offline using Matlab programs. The encrypted signal was then loaded into an arbitrary waveform generator (AWG), which had a sample rate of 10 Gs/s of electrical OFDM signal generation. A continuous-wave (CW) laser ($\lambda = 1550.3$ nm) was applied as the optical carrier. After that, the electrical signal in AWG was changed into optical by an optical Mach-Zehnder modulator (MZM). Thus, the net data rate applied was actually at 8.9 Gb/s (10 Gs/s × 4 × 64/256 × 8/9), with the electrical bandwidth of 2.5 GHz (10 Gs/s × 65/256). At ONU, the received data were recorded with a 20 Gs/s real-time oscilloscope after direct detection via a 10-GHz photodiode (PD). The waveform, electric and optical spectra of OFDM signals are measured and plotted in **Figure 10**.

The CCDFs of encrypted OFDM signals are plotted in **Figure 11**, where 10,000 OFDM symbols with 16-QAM modulation format were employed. From **Figure 11** it can be noted that, by employing chaotic signal scrambling, significant PAPR reduction is achieved, with respect to the conventional OFDM transmission without any signal scrambling. The total number of sub-blocks and phase factors applied in PTS was $L = 4$ and $K = 2$ respectively, and the phase factor in SLM was $V = 4$.

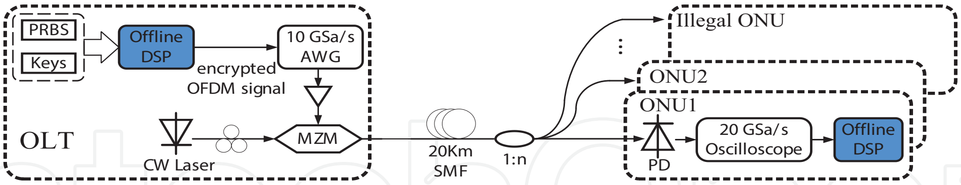


Figure 9. Experimental setup of encrypted OFDM transmission using chaotic PTS/SLM.

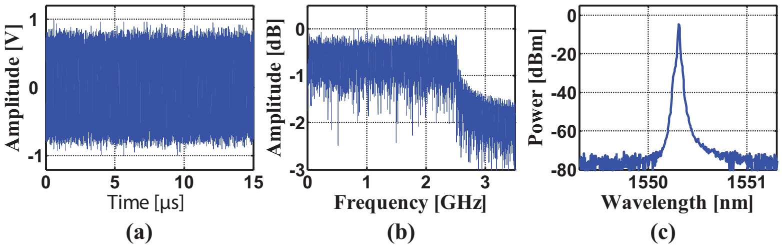


Figure 10. Encrypted OFDM signals. (a) Waveform; (b) electric spectrum; (c) optical spectrum.

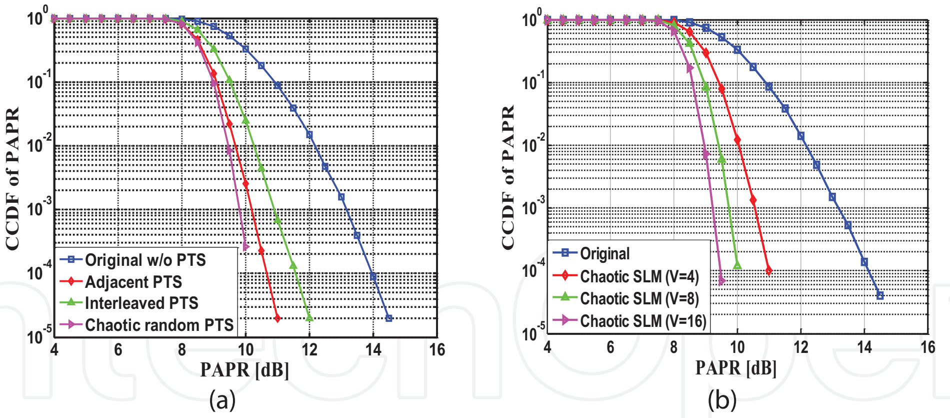


Figure 11. CCDFs of PAPR in chaotic (a) PTS; (b) SLM.

The bit error ratio (BER) measurements of secure OFDM transmission using chaotic PTS/SLM are plotted in **Figure 12**. The OFDM signals can be correctly decrypted after transmission over 20 km standard single-mode fiber (SSMF) for legitimate ONUs with the correct keys, while any illegal ONU cannot decrypt OFDM signals with a wrong key, which is even a tiny discrepancy of 1×10^{-15} away from the correct key. The corresponding constellations are plotted as the insets in **Figure 12**. If compared with the conventional OFDM transmission, the BER performance was improved ~1 dB (BER@10^{-3}) for encrypted OFDM signals, if compared with back-to-back (B2B) signals, which can mainly be attributed to the effective reduction of PAPR through the signal scrambling schemes, either chaotic PTS or SLM.

4.2. Chaotic precoding of OFDM signals

Matrix precoding is a set of typical approaches for PAPR reduction, which provides unique properties such as lower computational complexity and higher spectral efficiency (without requirement of sideband), if compared with the signal scrambling schemes. Actually, PAPR

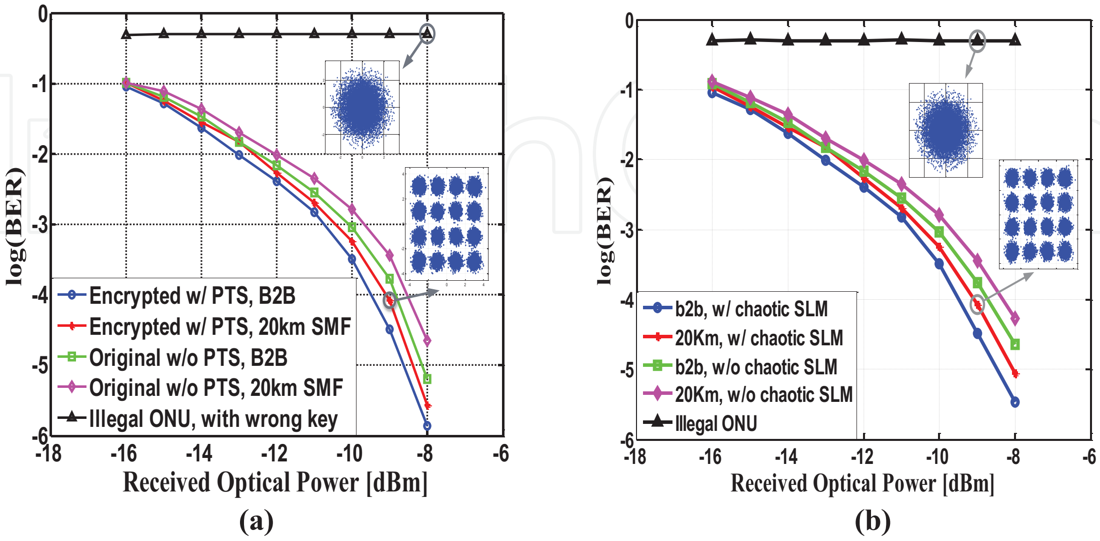


Figure 12. BERs of encrypted OFDM transmission using chaotic (a) PTS; (b) SLM.

reduction is achieved through the proper selection and distribution of power between OFDM blocks. In this section, the digital chaos will be employed into the precoding schemes, aimed to construct or reconfigure the standard precoding matrices into alternative chaotic ones, so that the security can be enhanced during transmission via the introduction of digital chaos into the procedure of OFDM signal precoding, and jointly the PAPR can be reduced.

4.2.1. Chaotic discrete Fourier transform spread OFDM (DFT-S-OFDM)

As depicted in **Figure 13**, the DFT-S-OFDM data encryption is implemented multi-fold, such as chaotic TS insertion, chaotic DFT matrix generation, and chaotic subcarrier allocation, all of which are predetermined by digital chaotic sequences [20]. The details of encryption are given as follows.

In the first fold of encryption, one chaotic sequence is used to generate TS, the same way as described in the previous chaotic signal scrambling schemes. The second fold of encryption is to generate the chaotic reconfigurable DFT precoding matrix. Assuming **F** is the standard $M \times M$ DFT matrix, the matrix element is given by

$$\mathbf{F}_{\alpha,\beta} = \frac{1}{\sqrt{M}} e^{-j2\pi(\alpha-1)(\beta-1)/M}, \; 0 \le \alpha, \beta \le M-1 \tag{15}$$

where α, β are the indexes of row and column, respectively. From Eq. (15), a reconfigurable matrix can be generalized

$$\mathbf{F}'_{\alpha,\beta} = \frac{1}{\sqrt{M}} e^{-j2\pi(\alpha-m)(\beta-n)/M}, \; 0 \le \alpha, \beta \le M-1 \tag{16}$$

where m, n are the real constants, which can be predetermined using chaotic sequences obtained in Eq. (5) as

$$m_{y,i} = \cdots + 10n_1 + n_2 + 0.1n_3 + 0.01n_4 + \cdots \tag{17}$$

where n_j donates the n_jth digit in the decimal part of y. Similarly, $\{n_{z,i}\}$ can be generated from $\{z_i\}$ in the same way as $\{m_{y,i}\}$.

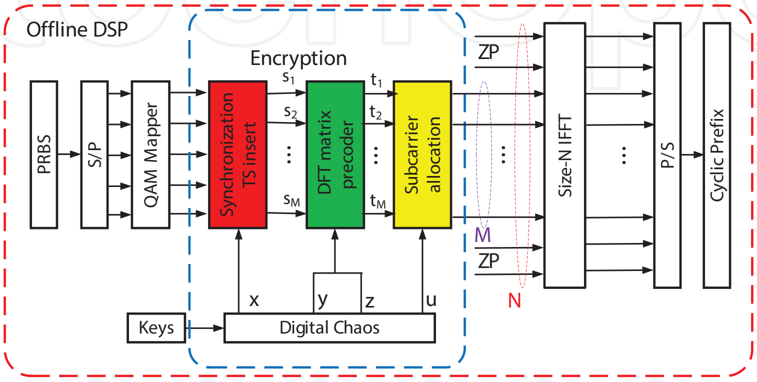


Figure 13. Schematic diagram of chaotic encrypted DFT-S-OFDM signal transmission.

Mathematically, the same basic features in the original standard **F** are kept for the reconfigurable DFT matrix **F**′. For example, the inverse matrix of **F**′ is equal to its conjugate matrix. Moreover, all of the elements in **F**′ are in geometric sequence with the same common ratio of $e^{-j2\pi/M}$ for the same row or column indexes.

To verify the capability of PAPR reduction of OFDM signals by the new DFT matrix **F**′, the upper bound of the peak factor should be considered, which is the square root of PAPR and depends on the aperiodic autocorrelation functions of the input symbols.

$$\gamma \leq 1 + \frac{2}{N}\sum_{n=1}^{N}|\rho_n| \tag{18}$$

$$\rho_n = \sum_{l=1}^{N-l} a_l a_{l+n}, \quad n = 1,\ 2, \ldots N-1 \tag{19}$$

where ρ_n are the aperiodic autocorrelation coefficients, a_n are the input symbols (QAM, QPSK, etc.), and N is the total number of subcarriers. Eq. (18) shows that, if the autocorrelation coefficients in the corresponding input symbols are small, the peak factor of OFDM signals will be small.

Assuming the kth OFDM symbol is $s^{(\mathrm{k})} \triangleq [s_1^{(\mathrm{k})}, s_2^{(\mathrm{k})}, \cdots, s_M^{(\mathrm{k})}]^T$, where T denotes the transpose of matrix, the DFT precoded OFDM signal becomes

$$\boldsymbol{t}^{(\mathrm{k})} \triangleq [t_1^{(\mathrm{k})}, t_2^{(\mathrm{k})}, \cdots, t_M^{(\mathrm{k})}]^T = \mathbf{F}'\boldsymbol{s}^{(k)} \tag{20}$$

As plotted in **Figure 14(a)**, the same non-periodic autocorrelation functions are obtained for the OFDM symbol $t^{(k)}$, either precoded with DFT matrix **F** or **F**′. From **Figure 14(a)**, it should be noted that different shapes of sidelobe appear in the autocorrelation functions, while the sidelobe shapes of OFDM signals with DFT precoding are lower than those without DFT precoding, when the same modulation format is applied. This verifies that, effective PAPR reduction of OFDM signals is achieved by DFT precoding with the reconfigurable matrix **F**′, the same effect as the standard DFT matrix **F**.

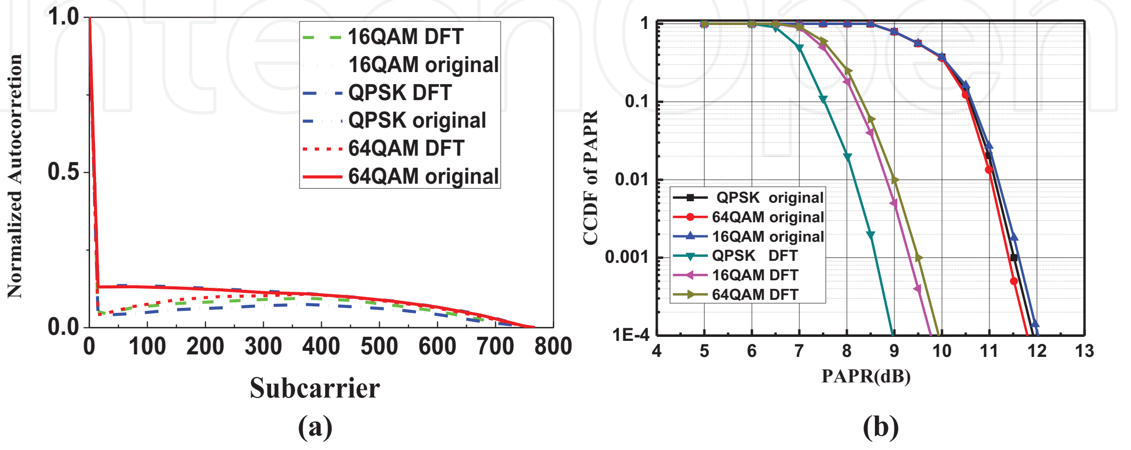


Figure 14. PAPR reduction using chaotic DFT, (a) normalized aperiodic autocorrelation function; (b) CCDFs of PAPR.

To directly evaluate the PAPR reduction, the CCDF curves is plotted in **Figure 14(b)**, for the cases of OFDM signals with and without the reconfigurable DFT precoding, where 100,000 OFDM symbols are applied in the formats of QPSK, 16-QAM, and 64-QAM, while Nyquist sampling rate is adopted. It can be observed that, if compared with the cases without DFT, the OFDM signals precoding with the reconfigurable matrix DFT can reduce the PAPR, regardless of the modulation formats, while the differences at the probability of 10^{-4} are about 3, 2.3, and 1.9 dB respectively for QPSK, 16-QAM, and 64-QAM. The CCDF curves in **Figure 14(a)** prove that, the new reconfigurable DFT does significantly reduce the PAPR of OFDM signals.

Finally, the fourth chaotic sequence $\{u_i\}$ is used to generate the scrambling criterion for subcarrier allocation before ZP. After an array $\{w_i\}$ $(i=1,\ldots,M)$ is obtained from $\{u_i\}$, where M is the total number of subcarriers (as shown in **Figure 13**), the elements in $\{w_i\}$ are swapped into $\{w_i'\}$ in the new order with respect to their values, for instance, from the lowest value to the highest. Then the new index order of subcarriers is rearranged as that of $\{w_i'\}$, details as shown in **Figure 15**. For example, assuming an original chaotic array of $\{0.8, 0.3, 0.5, 1.2, 1.1\}$, it is swapped from the small value to the big one, and then the new array $\{0.3, 0.5, 0.8, 1.1, 1.2\}$ can be obtained. In the original OFDM symbol, the first subcarrier is changed into the third position of the new OFDM symbol; similarly, the second is assigned to the first position, and so on. Following this scrambling criterion, a key space of $M!$ is created for OFDM data encryption.

The setup of IM/DD OFDM transmission experiment was the same as applied in the previous signal scrambling schemes; however, with the FFT points of 1024 and the number of subcarriers of 384, consequently the data rate was 13.3 Gb/s (10Gs/s×4×384/1024×8/9). The BER measurements were shown in **Figure 16**, for the encrypted 16-QAM OFDM signals. The encrypted signals with DFT-S-OFDM precoding were fully recovered by the legal ONUs. Due to the effective PAPR reduction via DFT precoding, the BER performance was improved ~2 dB (BER@10^{-3}) for the encrypted DFT-S-OFDM signals, if compared with the cases of original OFDM transmission without DFT precoding. The power penalty was only 0.9 dB (at BER@10^{-3}) between the case of B2B and transmission after 20 km SSMF. Moreover, for any illegal ONU with a wrong key, even a very small deviation of 1×10^{-15}, it was not possible to decrypt the original OFDM signals. The corresponding constellations for correct and incorrect chaotic keys are plotted as insets in **Figure 16**, which verified the security feasibility of chaotic DFT-S-OFDM signal transmission.

To quantitatively evaluate the performance dependence on the mismatches of row or column parameters $\Delta m, \Delta n$ in the reconfigurable DFT matrix $\mathbf{F}'$, the BERs are shown with respect to the parameters $\Delta m, \Delta n$ in **Figure 17**, where the modulation format is 16-QAM, and the received optical power is -9 dBm. In **Figure 17(a)**, when $\Delta m > 0.01$, the BER is significantly deteriorated

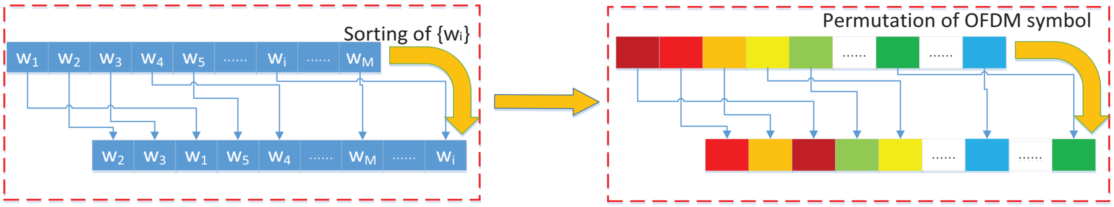


Figure 15. Subcarrier allocation in OFDM symbol using digital chaotic sequences.

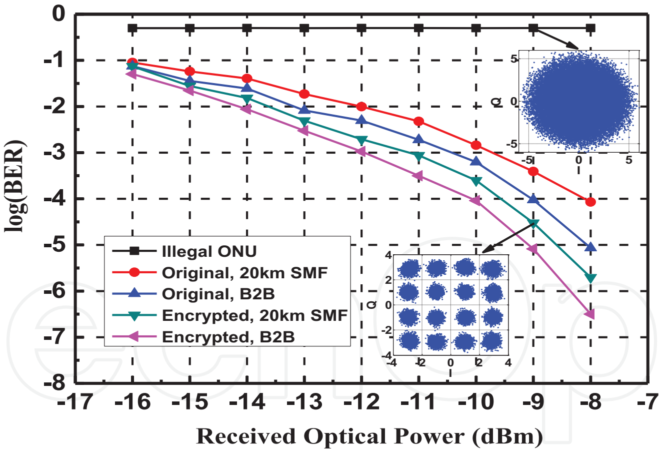


Figure 16. BERs of chaotic encrypted DFT-S-OFDM transmission.

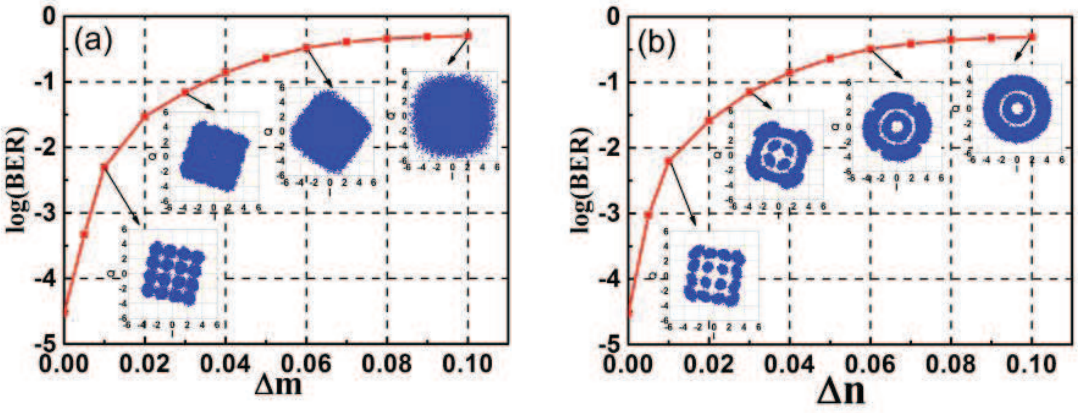


Figure 17. BERs versus the index mismatches in (a) Δm (b) Δn of chaotic DFT matrix.

(BER>10^{-3}), thus the data cannot be correctly received, even after using forward error correction approaches. It can also be noted that, if Δm is increased further, deterioration becomes more serious, as shown in the corresponding BERs and constellations. Similarly, the BERs variation with respect to the column parameter mismatch in the reconfigurable DFT matrix in $\mathbf{F}'$ is plotted in **Figure 17(b)**. From **Figure 17(b)**, the original data can be only recovered when $\Delta n < 0.01$. The results also verify that, the rotation angles in the corresponding constellations become larger with the increase of Δn. The difference of BERs and constellations with respect to $\Delta m, \Delta n$ again confirms that it is helpful to set two independent values of m, n in the new reconfigurable DFT matrix in $\mathbf{F}'$, for the purpose of key space expansion in encryption scheme using chaotic DFT precoding.

For the proposed multi-fold DFT-S-OFDM data encryption, the total key space can be given as follows. First, the parameters in DFT matrix (both of row and column) can be varied from 0 to 384 with the sensitivity of 0.01, which generates a key space of ~$1.5\times10^{9}(38,400\times38,400)$ for each OFDM symbol. Second, the subcarrier allocation generates a key space of 384!. Finally, the chaotic TS for OFDM symbol time synchronization enlarges the key space by a factor of ~10.

4.2.2. Chaotic Walsh-Hadamard transform (WHT)

Chaotic WHT is an alternative encryption technique using signal precoding, which provides lower computational complexity if compared with DFT precoding. The encryption scheme based on a reconfigurable chaotic WHT precoding matrix is shown in **Figure 18** [21], where the modified version of reconfigurable WHT matrix is also determined by digital chaos.

Theoretically, it can be proven that the permutation on the standard WHT matrix does not degrade the precoding properties. Since the WHT matrix is an orthogonal matrix whose elements are constrained from the set $\{-1, 1\}$,

$$\mathbf{H}\mathbf{H}^{\mathrm{T}} = \mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I} \tag{21}$$

Assuming $\mathbf{Q}_{n\times n}$ and $\mathbf{R}_{n\times n}$ are the row and column permutation matrices on WHT matrix $\mathbf{H}_{n\times n}$ respectively, then the chaotic row/column permutated WHT matrix becomes $\mathbf{P}_{n\times n}$.

$$\mathbf{P} = \mathbf{QHR}, \quad \mathbf{P}^{\mathrm{T}} = \mathbf{R}^{\mathrm{T}}\mathbf{H}^{\mathrm{T}}\mathbf{Q}^{\mathrm{T}} \tag{22}$$

$$\mathbf{P}\mathbf{P}^{\mathrm{T}} = \mathbf{QH}(\mathbf{R}\mathbf{R}^{\mathrm{T}})\mathbf{H}^{\mathrm{T}}\mathbf{Q}^{\mathrm{T}} = \mathbf{QHI}\mathbf{H}^{\mathrm{T}}\mathbf{Q}^{\mathrm{T}} = \mathbf{Q}n\mathbf{I}\mathbf{Q}^{\mathrm{T}} = n\mathbf{I} \tag{23}$$

To specify the PAPR reduction capability of chaotic WHT matrix, the same analysis based on the autocorrelation coefficient can be applied as for chaotic DFT.

As plotted in **Figure 19(a)**, the original 16-QAM OFDM symbols are applied and compared with the standard and chaotic WHT. The autocorrelation function is reduced in sidelobe if either chaotic or standard WHT is employed. An enlarged sidelobe for a specific zone is inserted in **Figure 19(a)** for clear view. Moreover, the sidelobe shape is exactly the same for both the standard and chaotic WHT precoders.

Furthermore, the CCDF curves are calculated for the cases of chaotic WHT, standard WHT, and un-precoded original OFDM signals, as shown in **Figure 19(b)**. The PAPR is effectively reduced by ~1 dB by either the standard or chaotic WHT precoder, compared to the un-precoded OFDM signals. In addition, the CCDFs are exactly the same for the standard and chaotic WHT, which again verifies the above theoretical analysis.

Therefore, row/column permutated WHT can be still applied as a precoder not only to reduce the PAPR but also to enhance the physical-layer security of OFDM data, since the correct

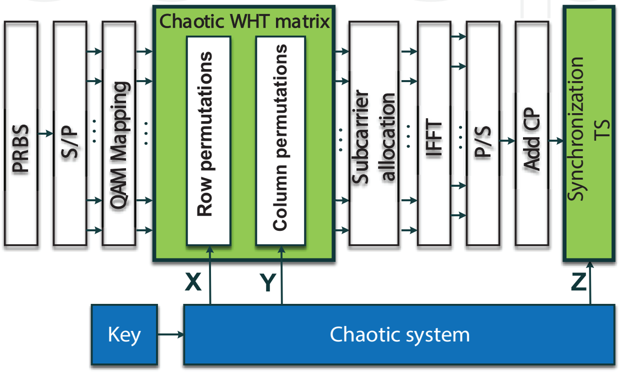
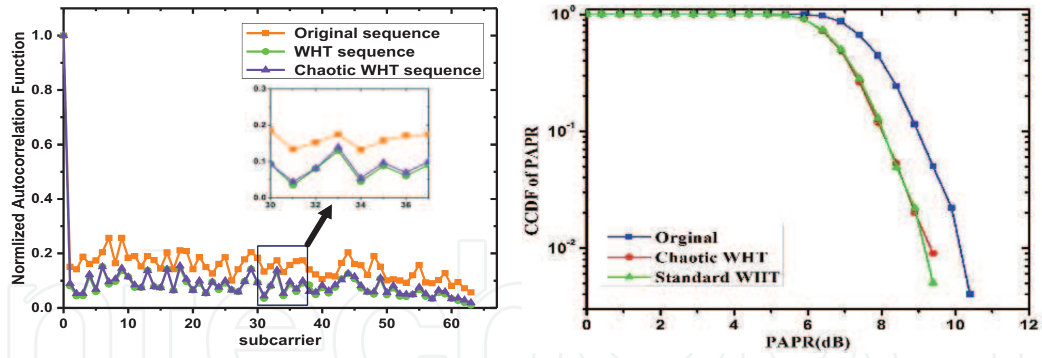


Figure 18. Schematic diagram of OFDM encryption precoded with chaotic WHT.



(a) (b)

Figure 19. PAPR reduction precoded by the standard/chaotic WHT, (a) normalized aperiodic autocorrelation function; (b) CCDF of PAPR.

original OFDM data can be recovered only after obtaining the correct row/column sequences to reconstruct the chaotic WHT matrix through legal ONUs.

In the proposed chaotic WHT scheme, a 3D hyper Chen's chaos is implemented to generate the digital chaotic sequences for data encryption [22]:

$$\begin{cases} \dot{x} = -ax + y \\ \dot{y} = (c-a)x + cy + xz \\ \dot{z} = bz + xy \end{cases} \tag{24}$$

where a, b, and c are constants. Generally, with a=35, b=3, $c\in$[20, 28.4], it enters into chaotic zones. To generate the permutation vectors D_x, D_y, and D_z, each of the chaotic sequences $\{x\}$, $\{y\}$, and $\{z\}$ is post-processed as follows.

First, we assume that the length of chaotic sequences $\{x\}$ and $\{y\}$ is M, where M is the order of WHT matrix, and then

$$D_x = sort\{x\}, \quad D_y = sort\{y\}, \quad D_z = sort\{z\} \tag{25}$$

where *sort* function returns an index vector, according to the ascending order of the values in the chaotic sequences.

The procedure of the proposed WHT chaotic encryption is given as follows. The two permutation vectors D_x and D_y, are used to permute the row and column indexes of the standard WHT matrix, respectively. Assuming the standard WHT matrix $\mathbf{H}^{(0)}_{M\times M}$ is

$$\mathbf{H}^{(0)}_{M\times M} = [\boldsymbol{r}^T_1, \boldsymbol{r}^T_2, \cdots, \boldsymbol{r}^T_M] \tag{26}$$

where r_1, $r_{2,\ldots,}$ r_M are the row vectors. After row permutation, it becomes

$$\mathbf{H}^{(1)}_{M\times M} = [\boldsymbol{r}^T_{\boldsymbol{Dx}(1)}, \boldsymbol{r_{Dx}}^{\boldsymbol{T}}{}_{(2)}, \cdots \boldsymbol{r_{Dx}}^{\boldsymbol{T}}{}_{(M)}] = [\boldsymbol{c}_1, \boldsymbol{c}_2 \cdots \boldsymbol{c}_M] \tag{27}$$

Similarly, the columns are permutated via vector D_y, and the corresponding chaotic WHT matrix after both row and column permutations becomes

$$\mathbf{H}^{(2)}_{M\times M} = [c_{D_y(1)}, c_{D_y(2)}, \cdots, c_{D_y(M)}] = [v_1^T, v_2^T, \cdots, v_M^T] \tag{28}$$

The chaotic sequence D_z is used to generate the chaotic TS for OFDM symbol synchronization, which is composed of random $\{-1, 1\}$ and defined as [23]

$$\mathrm{TS} = \{(\mathrm{mod}(D_{z,i},\ 2) - 0.5)\times 2\} \tag{29}$$

Since the hyper-chaotic sequences have high sensitivity to the initial values (~1×10^{-15}) and present exceptional random behavior, the initial values are served as the security key between OLT and ONUs. A secure channel has to be employed to transfer the keys between OLT and ONUs, for instance, using quantum key distribution (QKD), which is out of the scope of this chapter and will not be given in detail here. **Figure 20** shows the sensitivity of the row/column permutation indexes of chaotic WHT matrix with respect to a tiny change in the initial conditions.

Figure 21 shows the experimental setup of the encrypted transmission of OFDM signals using chaotic WHT precoding. The IM/DD was also applied, and the details were described in Section 4.1. At OLT, there were 256 points in IFFT, among which 64 subcarriers were used for OFDM data. The effective data rate was 8.9 Gb/s (10 Gs/s×4×64/256/(1+1/8)). The signal waveform, electric and optical spectra are plotted as insets in **Figure 21**.

The transmission performance was evaluated for OFDM signals precoded by chaotic WHT via BER measurements of 128 OFDM symbols, for the cases of B2B and transmission after 20 km

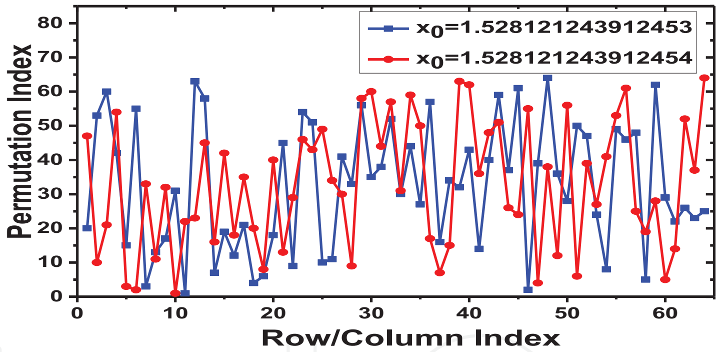


Figure 20. Chaotic permutation index versus a slight change in the initial values.

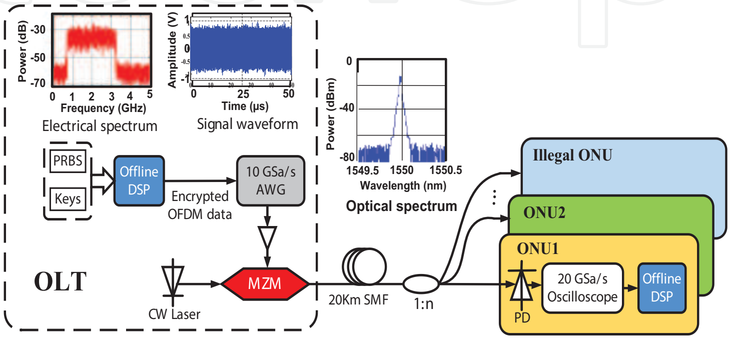


Figure 21. Experimental setup of encrypted optical OFDM transmission using chaotic WHT.

SSMF, as shown in **Figure 22**. The BER was improved by ~1 dB (BER@10^{-3}) in receiver sensitivity for chaotic WHT, compared with the un-precoded OFDM signals. This improvement can be mainly attributed to the precoding gain from chaotic WHT, since BER was improved also for the case of B2B, which verified the effective PAPR reduction in OFDM signals through chaotic WHT precoding. For transmission after 20 km SSMF, the effect of fiber dispersion is negligible due to the narrow spectrum of OFDM signals.

The robustness of the multi-fold data encryption is evaluated via the total key space created by chaotic WHT, since only legal ONUs can generate the correct chaotic WHT matrix to recover the original OFDM data. Assuming that the dimension of chaotic WHT matrix is 64 × 64, it creates a total key space of 64! × 64! (~10^{178}). In addition, the chaotic TS for OFDM symbol synchronization further increases the key space by a factor of ~10. As a result, a total key space of ~10^{179} is achieved in chaotic WHT encryption scheme.

The computational complexities the chaotic encryption schemes with PAPR reduction are listed in **Table 1**. The computational complexity is reduced significantly in WHT, since it does not require complex multiplication if compared with DFT, SLM, and PTS, because the elements in WHT matrix are constrained to the value set of {1,−1}. Meanwhile, WHT has the same

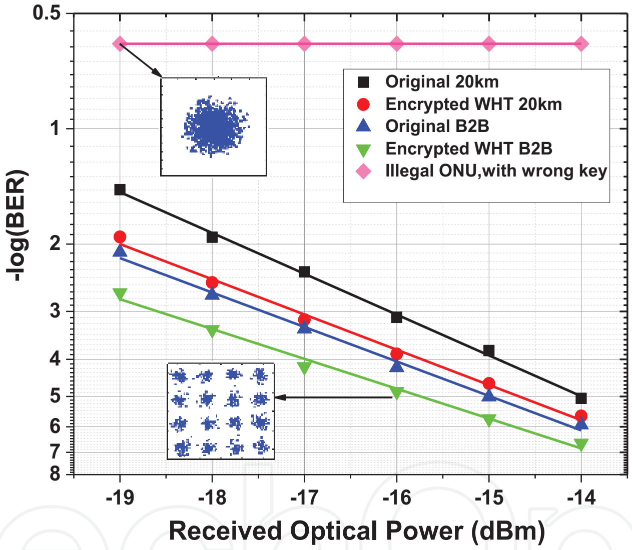


Figure 22. BER measurements of the OFDM transmission with and without chaotic WHT.

	WHT	DFT	SLM	PTS
Multiplication	None	N^2	$B\frac{\mathrm{gN}}{2}\log_2\mathrm{gN}$	$V\frac{\mathrm{gN}}{2}\log_2\mathrm{gN}$
Addition	$N(N-1)$	$N(N-1)$	$\mathrm{BgN}\ \log_2\mathrm{gN}$	$VgN\ log_2\ gN + (V-1)gNW^V$
Sideband	None	None	Needed	Needed

B is the number of candidate signals in SLM, *V* is the number of sub-blocks, and *W* is the number of phase factors.

Table 1. Computation complexity and sideband information of chaotic encryption schemes with PAPR reduction.

addition complexity as DFT. In addition, if compared with PTL or SLM schemes, simpler optical OFDM transmission structure and higher spectral efficiency can be expected for the WHT and DFT precoding schemes, since no additional sideband information needs to be transmitted.

5. Conclusions

We have reviewed a serial of novel data encryption schemes for physical-layer security enhancement for optical OFDM transmission. By incorporating multi-fold digital chaos-based data encryption in various DSP procedures in OFDM signal generation, modulation as well as OFDM symbol synchronization, data security is greatly enhanced with a huge key space. Moreover, the OFDM transmission performance is significantly improved because the pseudo-random properties of digital chaos are employed for effective PAPR reduction. Moreover, for the chaotic precoding schemes, the reconfigurable chaotic precoding matrices are predetermined by digital chaos; therefore, the sideband information is no longer necessary, which also improves the spectral efficiency in transmission. The proposed chaotic data encryption schemes have been successfully demonstrated by ~10 Gb/s OFDM transmission experiments, which verifies that these schemes could be promising candidates for next-generation secure OFDM-PON.

Acknowledgements

This work was supported in part by International S&T Cooperation Program of China, 2016YFE0104500, Natural Science Fund of China under Grants 61571291, 61431009, and 61221001.

Author details

Xuelin Yang*, Adnan A.E. Hajomer and Weisheng Hu

*Address all correspondence to: x.yang@sjtu.edu.cn

State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai, China

References

[1] Fang Y, Yu J, Zhang J, Chi N, Xiao J, Chang G. Ultrahigh capacity access network architecture for mobile data backhaul using integrated W-band wireless and free-space optical links with OAM multiplexing. Optics Letters. 2014;**39**(14):4168–4171. DOI: 10.1364/OL.39.004168

[2] Reis J, et al. Terabit+ (192 × 10Gb/s) Nyquist shaped UDWDM coherent PON with upstream and downstream over a 12.8 nm band. Journal of Lightwave Technology. 2014;**32**(4):729–735. DOI: 10.1109/JLT.2013.2283017

[3] ITU-T Recommendation G.983.1, Broadband Optical Access Systems Based on Passive Optical Networks, International Telecommunication Union-Telecommunication Sector (ITU-T); 2005

[4] Zhang L, Xin X, Liu B, Yin X. Physical secure enhancement in optical OFDMA-PON based on two-dimensional scrambling. Optics Express. 2012;**20**(26):B32–B37. DOI: 10.1364/OE.20.000B32

[5] Liu B, Zhang L, Xin X, Wang Y. Physical-layer security in OFDM-PON based on dimension-transformed chaotic permutation. IEEE Photonics Technology Letters. 2014;**26**(2):127–130. DOI: 10.1109/LPT.2013.2290041

[6] Zhang L, Xin X, Liu B, Wang Y. Secure OFDM-PON based on chaos scrambling. IEEE Photonics Technology Letters. 2011;**23**(14):998–1000. DOI: 10.1109/LPT.2011.2149512

[7] Liu B, et al. Piecewise chaotic permutation method for physical-layer security in OFDM-PON. IEEE Photonics Technology Letters. 2016;**28**(21):2359–2362. DOI: 10.1109/LPT.2016.2594042

[8] Zhang W, et al. Joint PAPR reduction and physical-layer security enhancement in OFDMA-PON. IEEE Photonics Technology Letters. 2016;**28**(9):998–1001. DOI: 10.1109/LPT.2016.2522965

[9] Zhang W, Zhang CF, Jin W, Chen C, Jiang N, Qiu K. Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON. IEEE Photonics Technology Letters. 2014;**26**(19):1964–1967. DOI: 10.1109/LPT.2014.2343616

[10] Yang X, Hu X, Shen Z, He H, Hu W, Bai C. Physical layer signal encryption using digital chaos in OFDM-PON. In: 10th International Conference on Information Communications and Signal Processing (ICICS); November 2015. DOI: 10.1109/ICICS. 2015.7459872

[11] Cvijetic N. OFDM for next generation optical access networks. Journal of Lightwave Technology. 2012;**30**(4):384–398. DOI: 10.1109/JLT.2011.2166375

[12] Popoola WO, et al. Pilot-assisted PAPR reduction technique for optical OFDM communication systems. Journal of Lightwave Technology. 2014;**32**(7):1374–1382. DOI: 10.1109/JLT.2014.2304493

[13] Jayalath ADS, Tellambura C. Reducing the peak-to-average power ratio of orthogonal frequency division multiplexing signal through bit or symbol interleaving. Electronics Letters. 2000;**36**(13):1161–1163. DOI: 10.1049/el:20000822

[14] Sharif M, Gharavi-Alkhansari M, Khalaj BH. On the peak-to-average power of OFDM signals based on oversampling. IEEE Transactions on Communications. 2003;**51**(1):72–78. DOI: 10.1109/TCOMM.2002.807619

[15] Tang L, Zuo Q, Cui W. Synchronization scheme using four-dimensional chaotic system for OFDM. Journal of Communication. 2010;**31**(1):73–84 (in Chinese).

[16] Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos. 2006;**16**(8):2129–2151. DOI: 10.1142/S0218127406015970

[17] Hu X, Yang X, Shen Z, He H, Hu W. Chaos-based partial transmit sequence technique for physical-layer security in OFDM-PON. IEEE Photonics Technology Letters. 2015;**27**(23):2429–2432. DOI: 10.1109/LPT.2015.2466092

[18] Cheng M, et al. Security-enhanced OFDM-PON using hybrid chaotic system. IEEE Photonics Technology Letters. 2015;**27**(3):326–329. DOI: 10.1109/LPT. 2014.2370757

[19] Hu X, Yang X, Hu W. Chaos-based selected mapping scheme for physical-layer security in OFDM-PON. Electronics Letters. 2015;**51**(18):1429–1431. DOI: 10.1049/el.2015.1261

[20] Shen Z, Yang X, He H, Hu W. Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos. IEEE Photonics Journal. 2016;**8**(3). DOI: 10.1109/JPHOT.2016.2564438

[21] Hajomer A A E, Yang X, Hu W. Chaotic Walsh–Hadamard Transform for Physical Layer Security in OFDM-PON. IEEE Photonics Technology Letters. 2017;**29**(6): 527–530. DOI: 10.1109/ LPT. 2017. 2663400

[22] Chen G, Ueta T. Yet another chaotic attractor. International Journal of Bifurcation and Chaos. 1999;**9**(7):1465–1466. DOI: 10.1142/S0218127499001024

[23] Wang X, et al. SSBI mitigation at 60GHz OFDM-ROF system based on optimization of training sequence. Optics Express. 2011;**19**(9):8839–8846. DOI: 10.1364/OE.19.008839