This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LPT.2016.2522965, IEEE Photonics Technology Letters

Joint PAPR Reduction and Physical Layer Security Enhancement in OFDMA-PON

Wei Zhang, Chongfu Zhang, *Senior Member, IEEE*, Chen Chen, Wei Jin and Kun Qiu

***Abstract*—For joint peak-to-average power ratio (PAPR) reduction and physical layer security enhancement, we propose a chaos IQ-encryption based optimal frame transmission technique in an orthogonal frequency-division multiple access-based passive optical network (OFDMA-PON). The chaos IQ-encryption technique is utilized to enhance the physical layer security. In encrypting, the In-phase (I) and Quadrature-phase (Q) parts of the Quadrature amplitude modulation (QAM) symbols are coded with two phase sequences separately, which are generated using a two-dimensional Logistic map. The encrypted OFDM symbols comprise an OFDM frame, and the frame with the minimum PAPR is transmitted to the optical network unit (ONU) side. Thus the transmitted OFDM signal is of joint low PAPR and high physical layer security. In the demonstration, 11.32Gb/s encrypted 16QAM OFDM signal has been experimentally transmitted over 25 km standard single mode fiber (SSMF) in an intensity-modulation/direct-detection (IM/DD) OFDMA-PON.**

***Index Terms*—Passive optical network (PON), orthogonal frequency-division multiple access (OFDMA), Quadrature amplitude modulation (QAM), chaos encryption**

I. Introduction

THE orthogonal frequency-division multiple access-based passive optical network (OFDMA-PON) has emerged as one of the most promising solution to meet the requirement of the next generation networks, for the inherent advantages such as high spectral efficiency, strong tolerance to fiber dispersion, flexible resource allocation and potentially low cost [1,2]. However, the basic OFDM signal is of high peak to-average power ratio (PAPR), as the individual subcarrier signals add up coherently to produce high peaks in the time domain. The high PAPR requires optical components with a wide linear range to accommodate for the signal variations and reduce the transmission performance of the OFDM signal [3]. Hence, high PAPR is one of main challenges in OFDMA-PON systems. Besides, in an OFDMA-PON system, the downstream signal is broadcasted to all the optical network units (ONUs). This leads the downstream signals is vulnerable to eavesdropping. Thus, the secure problem should be taken seriously into considerations [4].

Recently, a chaos based selected mapping (CSLM) technique was proposed to reduce the PAPR in an IM/DD OFDM system [5]. Some chaos based encryption methods, including chaotic scrambling and permutation [6], hyper-chaotic system and fractional Fourier transformation [7], chaos based IQ encryption method [8], etc., were proposed to enhance the physical layer security of OFDM-PON systems. Owing to the special chaos-related characteristics, such as ergodicity, pseudo randomness and high sensitivity to the initial values, etc., these encryption methods are of high physical layer security. However, these techniques are only proposed for PAPR reduction or physical layer security enhancement.

In this letter, we propose and experimentally demonstrate a chaos IQ-encryption based optimal frame transmission (IQ-OFT) technique for joint PAPR reduction and physical layer security enhancement in an OFDMA-PON system. The security is originated from chaos IQ-encryption process. Furthermore, the transmitted OFDM signal is of low PAPR which is effectively reduced by the OFT technique. Compared with the CSLM technique, OFT technique embeds the side information (SI) in the pilot to overcome the influence on data rate by SI. The pilot also is effectively utilized for channel estimation. The transmission of 11.32 Gb/s encrypted 16 quadrature amplitude modulation (16QAM) OFDM signal over 25 km standard single-mode fiber (SSMF) is experimentally demonstrated in an intensity modulation / direct detection (IM/DD) OFDMA-PON system, where the OFDM modulation and demodulation are achieved with offline DSP.

II. Principle

The schematic diagram of the secure OFDMA-PON system with IQ-OFT technique is illustrated in Fig. 1. After serial-to-parallel conversion (S/P) and QAM mapping, the mapped QAM symbols are encrypted using IQ-encryption technique. In encrypting, the symbols are split into In-phase (I) and Quadrature-phase (Q) parts and then multiplied by a pair of phase sequences separately, which can be expressed as

This work is supported partly by National Science Foundation of China No. 61571092, 61171045, 61301156, Open Fund of State Key Laboratory at Shanghai Jiao Tong University No. 2013GZKF031301, Program for New Century Excellent Talents in University No. NCET-13-0099, Fundamental Research Funds for the Central Universities (No. ZYGX2013J005, ZYGX2013J001), and the 111 Project (B14039).

W. Zhang, C. F. Zhang, W. Jin, K. Qiu are with the Key Laboratory of Optical Fiber Sensing and Communication Networks (Ministry of Education) and School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: cfzhang@uestc.edu.cn).

C. Chen is with the School of Electrical and Electronic Engineering, Nanyang Technological University, 637553, Singapore (e-mail: chen0884@e.ntu.edu.sg).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LPT.2016.2522965, IEEE Photonics Technology Letters

$$S_t(n) = \mathrm{Re}\left(C_t(n)\right)\cdot a_t(n) + j\cdot \mathrm{Im}\left(C_t(n)\right)\cdot b_t(n) \quad (1)$$

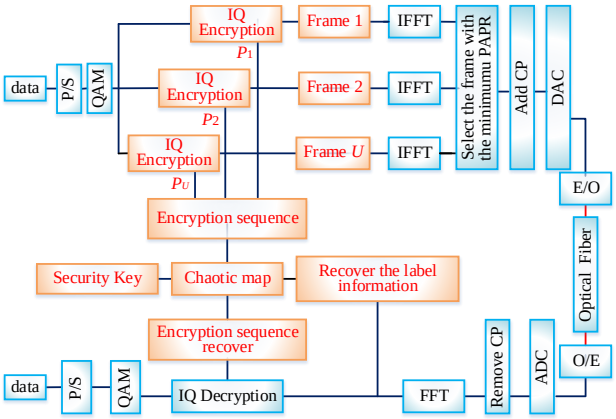

Fig. 1. The schematic diagram of the chaos IQ-OFT technique based secure OFDMA-PON system.

where $C_t(n)$ is the input QAM symbol on the n-th subcarrier at time t, n is the subcarrier index with n=1, 2,⋯, N, N is the number of the active subcarriers, t is the discrete time index, $a_t(n)$, $b_t(n) \in \{1, -1\}$ are the elements of two different encryption sequences P, Re(.) and Im(.) denotes the I and Q parts of the QAM symbol. After encrypting, the encrypted symbols $S_t(n)$, t=1, 2, …, T, n=1, 2, …, N, comprise an OFDM frame. T is the frame length, which is the number of the encrypted OFDM symbols in one frame. Meanwhile, pilot symbols are added for simultaneous label transmission and channel estimation. As an illustration, an OFDM frame is shown in Fig. 2. Using the unitary IFFT transform, the time domain OFDM signal can be expressed as (2)

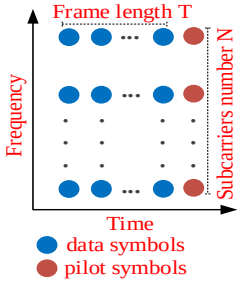

Fig. 2. An illustration of the pilot-assisted OFDM frame.

$$s_t(n) = \sum_{m=0}^{M-1} S_t(m)\cdot \exp\left(j\frac{2\pi nm}{M}\right), \quad 0 \le n \le M-1 \quad (2)$$

where M is the IFFT size. Then the PAPR value of the OFDM frame is calculated. The electrical PAPR of an OFDM frame in the time domain, is defined as

$$PAPR = \frac{\max\limits_{0\le n\le M(T+1)-1} \left|s_t(n)\right|^2}{E\left[\left|s_t(n)\right|^2\right]} \quad (3)$$

here E[.] denotes the statistical expectation. For selecting, the transmission data frame is encrypted U times using U different encryption sequences and comprise U OFDM frames. Each frame is of a corresponding pilot, which transmits the label of the encryption sequence. The pilot is from a pilot cluster, which is comprised of U different pilots. The pilot cluster is pre-generated by a chaotic map and stored at optical line terminal (OLT) and ONUs. Moreover, the pilot should be of low PAPR, since it is also considered in PAPR calculation. Then the encrypted OFDM frame with the minimum PAPR of all the U frames is transmitted to the ONUs side. At the ONU, after FFT, the stored pilot cluster is utilized to estimate the pilot of the received frame. The pilot with minimum error performance is extracted and the transmission pilot can be recovered. Then the recovered pilot is utilized to estimate the channel information, therefore the channel transfer matrix can be obtained. This is similar to the channel estimation technique via block-type pilot insertion mentioned in [9] and can effectively improve the quality of the transmitted OFDM signals. Furthermore, with the help of the recovered pilot and the security key, the corresponding encryption sequences can be recovered at ONUs to decrypt the downstream signal. The decryption principle is analogous to the encryption process

$$C_t(n) = \mathrm{Re}\left(S_t'\right)\cdot a_t(n) + j\cdot \mathrm{Im}(S_t')\cdot b_t(n) \quad (4)$$

here, S_t' is the output symbol of the FFT. For lack of the pilot and key information, the illegal ONU cannot recover the encryption phase sequence. Thus it cannot eavesdrop any useful information from the downstream signal.

The encryption sequences are generated by a two-dimensional (2D) coupled Logistic mapping as in [10]

$$\begin{aligned} x_{i+1} &= \mu_1 x_i\left(1-x_i\right) + \gamma_1 y_i^2 \\ y_{i+1} &= \mu_2 y_i\left(1-y_i\right) + \gamma_2\left(x_i^2 + x_i y_i\right) \\ 2.75 &< \mu_1 < 3.4, 2.75 < \mu < 3.45 \\ 0.15 &< \gamma_1 < 0.21, 0.13 < \gamma_2 < 0.15 \end{aligned} \quad (5)$$

Here the generated sequences x and y are chaotic in interval (0, 1). The sensibility of 2D Logistic map to change of the initial value x_0 is illustrated in Fig. 3. It can be seen that with only a slight change ($\sim 1\times 10^{-15}$) of the initial values x_0, the chaotic state falls into two absolutely different chaotic orbits. To improve the statistical properties of the generated sequences, the following preprocessing is performed

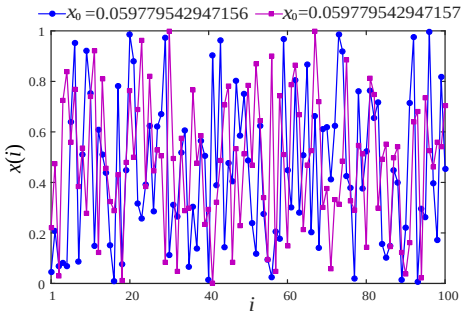

Fig. 3. The sensibility of 2D Logistic map to change of the initial value x_0.

$$\begin{aligned} x_i &= 10^6 x_i - floor(10^6 x_i) \\ y_i &= 10^6 y_i - floor(10^6 y_i) \end{aligned} \quad (6)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LPT.2016.2522965, IEEE Photonics Technology Letters

The generated sequence x and y are used to generate the encryption sequences using (7)

$$a(i) = sign(x(i) - 0.5)$$
$$b(i) = sign(y(i) - 0.5) \quad (7)$$

The generated sequences a and b are used to encrypt the transmission information at OLT and decrypt the downstream signals at ONUs.

III. Experiment Setup

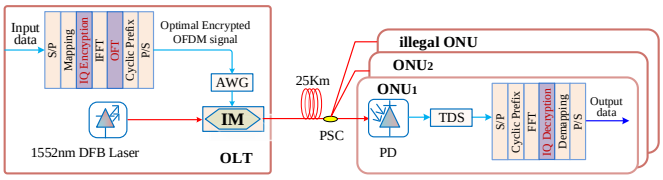

Fig. 4. Experimental setup of the proposed secure OFDM-PON (IM: intensity modulator, PSC: power splitter/coupler, PD: photodiode).

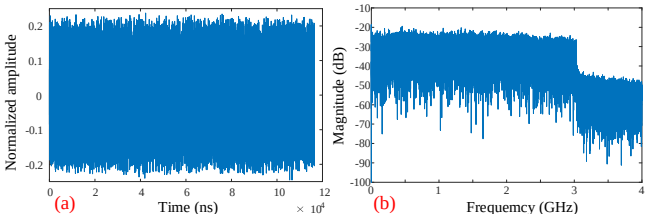

Fig. 5. (a) Electrical signal waveforms of the transmitted OFDM signal, and (b) electrical spectra of the received OFDM signal.

The experimental setup of the OFDMA-PON system is shown in Fig. 4, which comprises of the OLT, two regular ONUs and one illegal ONU. Two regular ONUs occupy different subcarriers and the illegal ONU eavesdrops the downstream signal from the ONU_1. Firstly, the pseudorandom binary sequence (PRBS) downstream data with a length of 2^{17}-1 are sent to the OFDM transmitter. Then S/P conversion, mapping, IQ-encryption, IFFT, selecting optimal frame, adding cyclic prefix (CP) and P/S conversion are performed in MATLAB. Here the modulation format is 16QAM. The frame length is T=5, while U=8. The IFFT size is 1024 and 308 active subcarriers are utilized to transmit valid data. The even and odd subcarriers are for ONU_1 and ONU_2, respectively. To ensure time domain signal comprises of real values only, the Hermitian symmetry is exploited. To avoid dispersion, the duration of the CP is 1/16 of the OFDM symbol duration. The optimal encrypted signal is loaded into an arbitrary waveform generator (AWG7102) with a sample rate of 10GSa/s. The total bit rate is calculated by R= $308\times4\times10/(1024\times(1+1/16))$ =11.32Gb/s. The output OFDM signal from the AWG is utilized to control the intensity modulator (IM), which works at 4.9V with a half-wave voltage of 8V. A 1550 nm distributed feedback (DFB) laser is used as the light source. The modulated optical signal is directly sent into the 25 km standard single mode fiber link (SSMF-28) and the launched optical power is 1.9 dBm. At the receiver, the optical OFDM signal is injected into a commercial PIN photodiode (PIN-PD) with a 3-dB bandwidth of 10 GHz to realize optical-to-electrical conversion. The detected electrical OFDM signal is sampled by a real time sampling scope (TDS) with a sample rate of 20 GSa/s. The signal decryption and demodulation are executed offline by MATLAB. The electrical waveforms of the transmitted OFDM signal and the power spectra of the received OFDM signal are shown in Figs. 5(a) and (b), respectively. We can see that the bandwidth of the transmission signal is about 3 GHz.

IV. Results and Discussion

The self-correlation and cross-correlation functions of the chaotic encryption sequences are calculated. Here, for encryption sequences a_h and a_j with length L, the normalized self-correlation and cross-correlation functions are defined as

$$R_{ac}(\tau) = \frac{1}{L}\sum_{l=0}^{L-1} a_j(l)a_j(l+\tau), -(L-1) \le \tau \le L-1$$
$$R_{cc}(\tau) = \frac{1}{L}\sum_{l=0}^{L-1} a_h(l)a_j(l+\tau), -(L-1) \le \tau \le L-1 \quad (8)$$

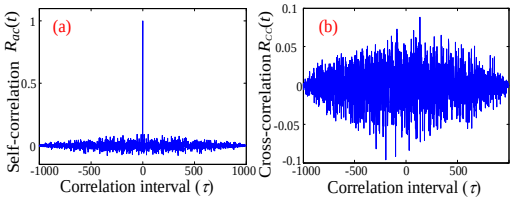

Fig. 6. The statistical correlation curves of chaotic sequence. (a) Self-correlation curves of chaotic sequence a_j; (b) Correlation curves of chaotic sequences a_j and a_h.

The statistical correlation curves of the generated encryption sequence are illustrated in Fig. 6. The initial values x_0 for a_h and a_j are 0.059779542947156 and 0.059779542947157, respectively. From Fig. 6(a), we can see that the value of the self-correlation functions of the sequences a_j are around zero with $\tau \neq 0$. From Fig. 6(b), the values of cross-correlation functions are also around zero for all values of τ. The results indicate that the generated encryption sequences have good correlation characteristic properties. Moreover, the generated encryption sequences also are sensitive to the initial values.

The secret keys of the system are expressed as {x_0, y_0, μ_1, μ_2, γ_1, γ_2}. It has been shown in Fig. 6 that the encryption sequences are sensitive to 10^{-15} difference for x_0. Thus, for a conservative estimate, the key space of the proposed encryption scheme is 5.46×10^{86} ($1\times1\times0.65\times0.7\times0.06\times0.02\times10^{15\times6}$). For current computing speed $3.38\times10^{17}s^{-1}$, it will take 1.61×10^{69} years to obtain the correct keys of the encryption sequence. Hence the key space can guarantee that the IQ-OFT technique successfully resist the exhaustive attack, which breaks a cipher by trying all possible keys. Furthermore, the pilot information and iterate time also introduces extra security to the encryption scheme. Additionally, for one frame, the IFFT calculation times of the IQ-OFT technique and CSLM technique are equal. For one QAM symbol, the IQ-OFT technique needs two real multiplications and one real addition and CSLM technique needs one complex multiplication. Therefore, the computational complexity of IQ-OFT technique is equal to the CSLM technique.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LPT.2016.2522965, IEEE Photonics Technology Letters

Fig. 7 illustrates CCDF curves of the original OFDM signal, the OFDM signal using IQ-OFT technique with different frame length *T*. As we can see the $PAPR_0$ at a CCDF of 10^{-4} for the IQ-OFT technique reduced above 2.8 dB compared with the original OFDM signal. With the increasing of the frame length *T*, the IQ-OFT technique's $PAPR_0$ at CCDF=10^{-4} increases. It should be note that when T =1, the IQ-OFT technique is analogous to the CSLM technique with the side information (SI) contained in the pilot. For comparison, the CCDF of the CSLM technique is also shown in Fig. 7. The CSLM technique's $PAPR_0$ at CCDF=10^{-4} is above 0.5 dB less than IQ-OFT technique. However embedding a pilot sequence within an OFDM frame does lead to a reduction of $1/(T+1)$ data rate. The data rate reduction ratio with different frame length *T* is Table I. With *T* increasing the data rate reduction ratio reduces. Comprehensive considering the PAPR reduction and data rate reduction, we set T =5 in the experiment. Although this introduces data rate reduction, the pilot insertion is contributed to improve the quality of the transmitted OFDM signals and establish the secure transmission. Thus the data rate reduction caused by pilot insertion can be acceptable.

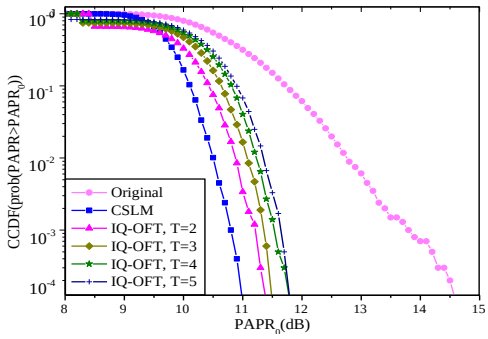

Fig. 7. CCDF curves of the original OFDM signal, the OFDM signal with CSLM technique and IQ-OFT technique.

TABLE I
DATA RATE REDUCTION RATIO PER FRAME

	CSLM	IQ-OFT			
		T=2	*T*=3	*T*=4	*T*=5
SI	50%	33%	25%	20%	16%

We have measured the error ratio (BER) performance of both illegal and regular ONUs which is illustrated in Fig. 8. It is observed that for two legal ONUs, the original data have been well recovered after decryption and demodulation. Compared with the original OFDM signal, the OFDM signal with IQ-OFT technique achieves about 1.6dB receiver power sensitivity improvements at a BER of 10^{-3} for both ONU_1 and ONU_2, contributed by the reduction of PAPR. This indicates that the transmission performance of the OFDM signal is effectively improved by the IQ-OFT technique. The received constellation diagram at the received optical power of -9dBm at ONU_1 is shown in inset of Fig. 8. The illegal ONU eavesdrops on the transmission information of the ONU_1 with a random security key. The BER is about 0.5, which indicates that no useful information from the downstream signal is eavesdropped.

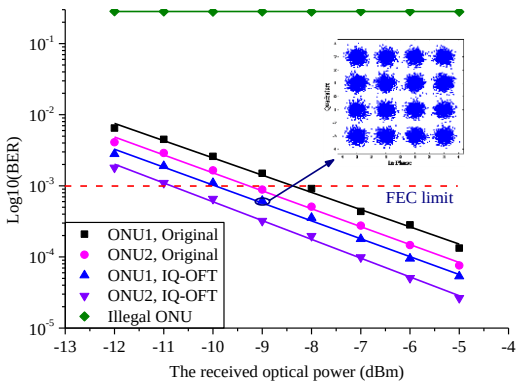

Fig. 8. BER performance and the corresponding constellations of 16-QAM

V. CONCLUSION

We have proposed a novel chaos IQ-encryption based optimal frame transmission technique in an OFDMA-PON. 11.32 Gb/s 16QAM OFDM signals with the IQ-OFT technique have been successfully implemented to verify the feasibility of our proposal. The obtained results prove that the OFDM signal with IQ-OFT technique is of joint low PAPR and high physical layer security. Compared with CSLM technique，the IQ-OFT technique has low data rate reduction and equivalent computation complexity. Furthermore, since the IQ-OFT technique only changes the phase of the QAM symbols, adaptive modulation techniques are compatible (power, bit, etc.) with the proposed IQ-OFT based OFDMA-PON system. Thus, the proposed IQ-OFT technique is quite promising for the future OFDMA-PON systems.

REFERENCES

[1] D. Nesset, "NG-PON2 technology and standards," *J. Lightwave Technol.*, vol. 33, no.5, pp. 1136-1143, Jan. 2015.

[2] C. Chen, C. F. Zhang, Y. Feng, and K. Qiu, "Bidirectional RF up-converted OFDMA-PON with novel source-free ONUs using FWM in SOA," *IEEE Photon. Technol. Lett.*, vol. 24, no. 4, pp. 2206-2209, Feb. 2012.

[3] W. Q. Popoola, Z. Ghassemlooy, B. G. Stewart, "Pilot-assisted PAPR reduction technique for optical OFDM communication systems," *J. Lightwave Technol.*, vol. 32, no. 7, pp. 1374-1382, Apr. 2014.

[4] M. Cheng, L. Deng, X. Gao, H. Li, "Security-enhanced OFDM-PON using hybrid chaotic system," *IEEE Photon. Technol. Lett.*, vol. 27, no. 3, pp. 326–329, Feb. 2015.

[5] Y. Xiao, M. Chen, F. Li, J. Tang, Y. Liu, L. Chen, "PAPR reduction based on chaos combined with SLM technique in optical OFDM IM/DD system," *Optical Fiber Technol.*, vol. 21, pp. 81-86, 2015.

[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. Deng, M. Cheng, X. Wang, H. Li, M. Tang, S. Fu, P. Shum, and D. Liu, "Secure OFDM-PON system based on chaos and fractional Fourier transform techniques," *J. Lightwave Technol.*, vol. 32, pp. 2629-2635, Jun. 2014.

[8] W. Zhang, C. F. Zhang, W. Jin, C. Chen, N. Jiang, and K. Qiu, "Chaos coding based QAM IQ-encryption for improved security in OFDMA-PON," *IEEE Photon. Technol. Lett.*, vol. 26, no. 19, pp. 1964–1967, Jul. 2014.

[9] L. Liu, X. Yang, and W. Hu, "Experimental evaluation of pilot pattern design in direct-detection optical OFDM transmission," Opt. Commun., vol. 294, pp. 83-87, May. 2013.

[10] X. Wang, Q. Shi, "New type crisis: hysteresis and fractal in coupled logistic map," Chin. J. Appl. Mech., vol.4, pp.501-506, 2005.