<table>
<thead>
<tr>
<th>Title</th>
<th>Joint PAPR Reduction and Physical Layer Security Enhancement in OFDMA-PON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Zhang, Wei; Zhang, Chongfu; Chen, Chen; Jin, Wei; Qiu, Kun</td>
</tr>
<tr>
<td>Citation</td>
<td>Zhang, W., Zhang, C., Chen, C., Jin, W., &amp; Qiu, K. Joint PAPR Reduction and Physical Layer Security Enhancement in OFDMA-PON. IEEE Photonics Technology Letters, 28(9), 998-1001.</td>
</tr>
<tr>
<td>Date</td>
<td>2016</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/40550">http://hdl.handle.net/10220/40550</a></td>
</tr>
<tr>
<td>Rights</td>
<td>© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<a href="http://dx.doi.org/10.1109/LPT.2016.2522965">http://dx.doi.org/10.1109/LPT.2016.2522965</a>].</td>
</tr>
</tbody>
</table>
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, 11.32 Gb/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 the 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
\[ S_i(n) = \text{Re}(C_i(n)) \cdot a_i(n) + j \cdot \text{Im}(C_i(n)) \cdot b_i(n) \] (1)

\[ C_i(n) = \text{Re}(C_i(n)) \cdot a_i(n) + j \cdot \text{Im}(C_i(n)) \cdot b_i(n) \] (2)

\[ S_i(n) = \sum_{m=0}^{M-1} S_i(m) \cdot \exp \left\{ j \frac{2\pi nm}{M} \right\}, \quad 0 \leq n \leq M - 1 \] (3)

\[ \text{PAPR} = \max_{0 \leq n < M} \left\{ \frac{1}{E[|S_i(n)|^2]} \right\} \] (4)

Here, \( S_i(n) \) 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]

\[ x_{i+1} = \mu_1 x_i (1 - y_i) + \gamma_1 y_i \] \( x_0 = 0.059779542947156 \)

\[ y_{i+1} = \mu_2 y_i (1 - x_i) + \gamma_2 (x_i^2 + x_i y_i) \] \( y_0 = 0.059779542947157 \)

\[ 2.75 < \mu_i < 3.4, 2.75 < \mu_i < 3.45 \]

\[ 0.15 < \gamma_i < 0.21, 0.13 < \gamma_i < 0.15 \]

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 (~1×10\(^{-15}\)) 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

\[ x_i = 10^6 x_i - \text{floor}(10^6 x_i) \]

\[ y_i = 10^6 y_i - \text{floor}(10^6 y_i) \] (5)

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

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

Fig. 3. The sensibility of 2D Logistic map to change of the initial value \( x_0 \).
The generated sequence \( x \) and \( y \) are used to generate the encryption sequences using (7)
\[
a(i) = \text{sign}(x(i) - 0.5) \\
b(i) = \text{sign}(y(i) - 0.5)
\] (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

![Experimental setup of the proposed secure OFDM-PON](image)

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 ONU1. 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 11.32Gb/s. The output OFDM signal from the AWG is 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 \( a_0 \) and \( a_j \) with length \( L \), the normalized self-correlation and cross-correlation functions are defined as
\[
R_{cc}(\tau) = \frac{1}{L-1} \sum_{\tau=0}^{L-1} a_j(l) a_j(l+\tau), -(L-1) \leq \tau \leq L-1 \\
R_{ac}(\tau) = \frac{1}{L-1} \sum_{\tau=0}^{L-1} a_j(l) a_j(l+\tau), -(L-1) \leq \tau \leq L-1
\] (8)

The statistical correlation curves of the generated encryption sequence are illustrated in Fig. 6. The initial values \( x_0 \) for \( a_0 \) 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 \( \tau \). 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 \( \{x_0, y_0, \mu_1, \mu_2, \gamma_1, \gamma_2\} \). 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 \( 5.46 \times 10^{46} \) (\( 1 \times 10^{0.05} \times 0.7 \times 0.06 \times 0.02 \times 10^{1546} \)). For current computing speed \( 3.38 \times 10^{17} \) s\(^{-1} \), it will take \( 1.61 \times 10^{69} \) years to obtain the correct keys of the encryption sequence.

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.
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.

![CCDF curves of the original OFDM signal, the OFDM signal with CSLM technique and IQ-OFT technique.](image1)

**Table I**

<table>
<thead>
<tr>
<th>DATA RATE REDUCTION RATIO PER FRAME</th>
<th>CSLM</th>
<th>IQ-OFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI</td>
<td>50%</td>
<td>33%</td>
</tr>
</tbody>
</table>

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 ONU1 and ONU2, 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 ONU1 is shown in inset of Fig. 8. The illegal ONU1 eavesdrops on the transmission information of the ONU1 with a random security key. The BER is about 0.5, which indicates that no useful information from the downstream signal is eavesdropped.

![BER performance and the corresponding constellations of 16-QAM.](image2)

**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**