Secure OFDM-PON Bandwidth-limited System Precoded by Chaotic Frank Sequence-Based Circulant Matrix

Geyang Wang, Peiji Song, Ying-yu Pan, Chun-Kit Chan, and Lian-Kuan Chen
Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong SAR, China
e-mail address: lkchen@ie.cuhk.edu.hk

Abstract: We propose chaotic frank sequence-based circulant matrixes with ~10^{88} key space. Encryption of 21.67-Gb/s-20km bandwidth-limited OFDM-PON has been experimentally demonstrated, which confirms the superior performance of the proposed scheme over the chaotic-DFT and chaotic-DHT. © 2023 The Author(s)

1. Introduction

Orthogonal frequency division multiplexing passive optical network (OFDM-PON) is emerging as a promising solution to meet the demand for higher capacity broadband services in future access networks for its inherent advantages, including simplicity, high tolerance to fiber dispersion, and high spectrum efficiency. However, with the broadcasting nature in the downstream link of the OFDM-PON systems, the information integrity is more susceptible to both eavesdroppers and illegal optical network units [1]. Simultaneous improvement of capacity and security in OFDM-PON systems is therefore becoming more challenging [2, 3]. The Chaotic-Discrete Hartley Transform (DHT) and Chaotic-Discrete Fourier Transform (DFT) have been proposed to reconfigure the standard precoding/spreading matrix to jointly enhance capacity and security. However, the high-frequency fading effect is severe in high-capacity OFDM-PON systems because of chromatic dispersion and devices' bandwidth limitation [4]. In [2, 3], the effects of bandwidth limitation in their proposed schemes have been addressed but limited. In this paper, a new chaotic frank-sequence (FS) based circulant matrix (CrM) is proposed and shows superior performance in bandwidth-limited scenarios than the conventional Chaotic-DFT-OFDM and Chaotic-DHT-OFDM. Experiments of a 21.67-Gbit/s, 20-km secure OFDM-PON system having ~10^{88} key space (KS) under 2.5-GHz bandwidth limitation are demonstrated. Note that by random (i) row, (ii) column, and (iii) phase permutation of the precoding matrix in transmission, the physical-layer key space (PKS) is ~1.2×10^{403} and it will be elaborated in the following.

2. Principles and experimental setup

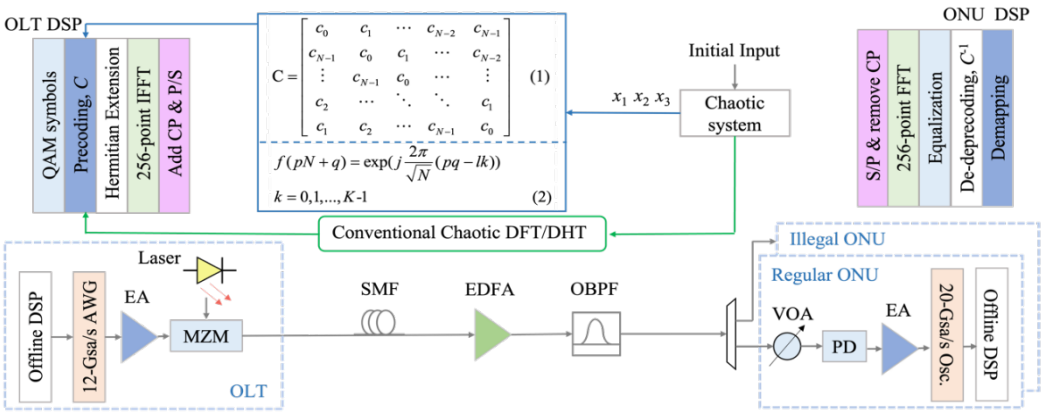

Fig. 1. Block diagram and the experiment setup of chaotic precoding-based OFDM-PON. (AWG: arbitrary waveform generator. EA: electrical amplifier. MZM: Mach-Zehnder modulator. SMF: single-mode fiber. EDFA: erbium-doped fiber amplifier. OBPF: optical bandpass filter. VOA: variable optical attenuator. PD: photodiode.)

Fig. 1 depicts the block diagram and experimental setup of the proposed secure OFDM-PON system using the chaotic precoding matrix. A random bit sequence is created and transferred to 16-QAM-modulated OFDM symbols S at the transmitter. The precoded signal A is then obtained by multiplying S with an *N*x*N* matrix C, i.e., A = CS where *N* is the number of payload subcarriers and is set to 121 in this paper. A frank sequence [5] based CrM, instead of the chaotic-DHT and -DFT matrices, is used for matrix C, which is created by circularly right shifting a basic *N*-element frank sequence $c = [c_0, c_1, ..., c_{N-1}]$, as illustrated by Eq. (1). The frank sequence is given in Eq. (2), where $\{p, q \in 0, 1, \ldots, (\sqrt{N}\text{-}1)\}$, $l = 0.6$ represents the minimum interval between two adjacent phases, and K satisfies $l \cdot K = \sqrt{N}$. Then

the time-domain signal can be obtained through Hermitian Extension, 256-point IFFT, cyclic prefix(CP) addition, and parallel-to-serial (P/S) conversion. At the receiver side, the reverse digital signal processing (DSP) process is performed, in which a digital filter with a 3dB bandwidth of 2.5 GHz is used to simulate the bandwidth limitation induced by components. In Fig. 1, the experimental setup is shown with a net data rate of ~21.67-Gb/s (=12-Gs/s×4 ×(121/256)/(1+12/256)). The proposed multi-dimension encryption scheme employs row/column permutations of the standard FS-based CrM and the chaotic phase parameter of frank sequence k. Specifically, we iterate the state equation of the chaotic system by the Runge-Kutta method [6] to acquire chaotic sequences of x_1, x_2, and x_3. Then the chaotic vectors p_1, p_2, and p_3 for row permutation, column permutation, and the chaotic phase parameter, respectively, can be generated by: $p_i = sort(\mathrm{mod}((|x_i| - floor(|x_i|)) \times 10^{15}, Q_i))$, i=1, 2, and 3, where $Q_1 = Q_2 = N$ and $Q_3 = K$. The function $sort(\cdot)$ generates an index vector in descending order. As only legitimate ONUs has the correct CrM to recover the original OFDM data, the resilience of the proposed encryption can be measured using the total KS obtained by the chaotic system. Based on [6], with initial inputs and parameters changed by 10^{-15} and/or 10^{-14}, respectively, the BER increases rapidly to ~0.5, resulting in a chaotic KS ~10^{88}. Actually, in transmission, the random permutation of 121 row/column and 18 phases provides a total permutation of $(121!)^2 \times 18 \sim 1.2 \times 10^{403}$ for PKS. The key space in this paper is claimed to be the chaotic KS, the smaller of KS and KPS, for the worst-case scenario as eavesdroppers may defalcate the permutation algorithms.

3. Experimental results and discussions

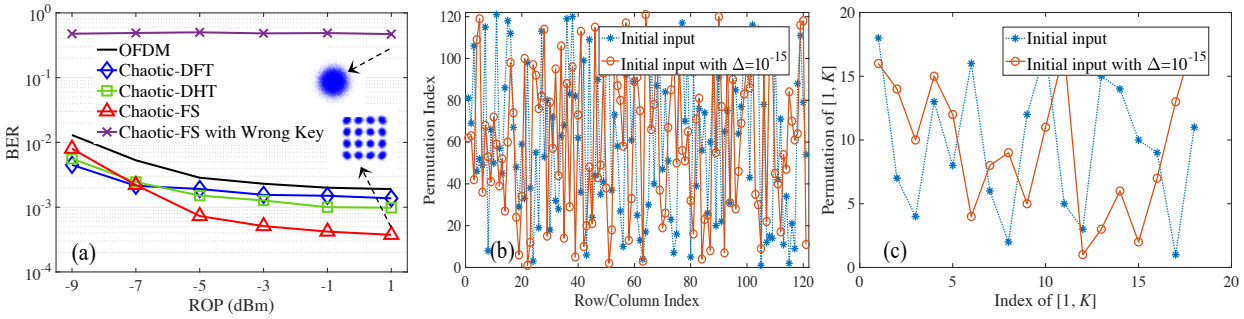

Fig. 2. (a) BER versus ROP using different security schemes and the constellation diagrams using the right key as well as the wrong key, respectively. (b) and (c) shows the sensitivity of the designed chaotic system in the case of p_1, p_2, and p_3 with tiny different initial inputs.

Fig. 2(a) shows the BER versus received optical power (ROP) with different encryption methods. In order to evaluate the performance improvement by the precoding matrix, encryption is only applied to the precoding matrix in each chaotic method. Clearly, the conventional chaotic-DFT and chaotic-DHT only have slight improvement compared with the original OFDM in the bandwidth-limited scenario. With the correct key, the proposed chaotic FS scheme outperforms the other two schemes, attributing to its satisfaction with the construction of discrete circulant transform precoding having a re-distribution of ISI/ICI power [7]. Conversely, illegal ONUs with the wrong key has a BER of ~0.5. In addition, the inset of Fig. 2(a) shows the corrupted constellations with the wrong key, indicating that no valid data can be derived. The encryption dimension used in our scheme includes (i) row permutation, (ii) column permutation, and (iii) a random phase parameter k. Then, the sensitivity of the initial keys is evaluated. Fig. 2(b) and 2(c) show the sensitivity of our chaotic system in terms of generated permutation vector $\{P_i\}$. Just a slight difference $\Delta=10^{-15}$ in initial input in these three cases [2]. This figure demonstrates drastically different permutation indexes from even a minute change in the initial input.

4. Conclusion

We have proposed a novel encrypted FS-based precoding secure OFDM-PON system. This chaotic system can obtain a huge key space of ~10^{88}, possibly extended to 1.2×10^{403}, to against the enumeration attack. A ~21.67-Gbit/s-20km secure OFDM-PON transmission with 2.5-GHz bandwidth limitation was experimentally demonstrated. It validates the superiority of the proposed scheme compared to conventional chaotic-DHT and -DFT. This work was partially supported by Hong Kong Research Grants Council (Project No. 14205820, 14204921)

5. Reference

[1] Z. Hu and C. -K. Chan, JLT, **36**(16), 3373-3381 (2018)
[2] A. A. E. Hajomer, X. Yang and W. Hu, PJ, **10**(2), 1-9 (2018)
[3] Z. Shen, X. Yang, H. He and W. Hu, PJ, **8**(3), 1-9 (2016)
[4] G. Wang, Z. Fan and J. Zhao, in Proc. OFC'2021, paper Tu1J4.
[5] R. Heimiller, Trans. Inf. Theory, **7**(4), 254-257 (1961)
[6] A. Sultan, X. Yang, et al., PTL, **30**(4), 339-342 (2018)
[7] J. Zhao, Y. Hong and L. -K. Chen, JLT, **37**(20), 5340-5353 (2019)