Chaotic Non-Orthogonal Matrix-Based Encryption for Secure OFDM-PONs

Zhouyi Hu, *Member, IEEE*, Peiji Song, *Student Member, IEEE*, and Chun-Kit Chan, *Senior Member, IEEE*

***Abstract*—We propose and experimentally demonstrate a novel encryption scheme to enhance the physical layer security in broadcast passive optical networks (PONs). We exploit, for the first time, a new dimension using non-orthogonality for encryption. Different from the conventional masking of data, the proposed chaotic non-orthogonal matrix (CNOM) can also dynamically scramble the number of subcarriers in an orthogonal frequency division multiplexing (OFDM) signal while maintaining the same bandwidth to further deceive potential eavesdroppers. By simultaneously using faster-than-Nyquist signaling and redundant precoding, the proposed scheme can achieve the compromise between spectral efficiency (SE) and resilience against system impairments, while increasing the overall key space. We then carry out a proof-of-concept experiment to verify the feasibility of the proposed CNOM-based encryption. Results showed that the transmission performance could be improved in addition to the security enhancement.**

***Index Terms*—Chaos encryption, orthogonal frequency division multiplexing (OFDM), passive optical networks (PONs).**

I. Introduction

PASSIVE optical networks (PONs) have been well-recognized as a promising “last mile” solution to realize the network goals of high capacity, high flexibility and low cost. However, in the conventional single-wavelength PON, the downstream data from an optical line terminal (OLT) is broadcasted to all the optical network units (ONUs) [1], making them very susceptible to possible eavesdropping. To resolve this issue, many encryption techniques have been proposed to enhance the physical-layer security in PONs. On the other hand, thanks to the high spectral efficiency (SE) and the robust digital signal processing (DSP), the applications of encryption to orthogonal frequency division multiplexing (OFDM) systems have been extensively investigated [2-8]. However, many of them only used primitive permutations for scrambling, which was far from satisfactory for encryption. In our previous work, we thus proposed a real-valued chaotic orthogonal matrix transform (RCOT) based encryption algorithm for secure OFDM-PONs [9]. By utilizing the chaotic behavior of the RCOT matrices, high randomness and unpredictability can be guaranteed.

In this letter, we extend the concept of RCOT to a more general case, and exploit it with our recently proposed non-orthogonal matrix precoding (NOM-p) [10] for security improvement in OFDM-PONs. In the proposed encryption scheme, the input data are scrambled by a set of chaotic non-orthogonal matrices (CNOMs), which are determined by a chaotic system and security keys. Compared to the chaotic orthogonal matrix (COM) -based encryption studied in our previous work [9], the proposed CNOM-based encryption provides a new dimension to deceive the potential eavesdroppers due to its deliberate violation of the orthogonality principle. Herein, faster-than-Nyquist (FTN) signaling [10] and redundant precoding [11] are both utilized to increase the key space and control the overall data rate. We, therefore, investigate the impact of its dynamic range in encryption on transmission and security performance. A proof-of-concept experiment is set up to emulate a broadcast OFDM-PON. By employing the proposed CNOM-based encryption, secure transmission can be guaranteed, and an additional coding gain is also demonstrated.

II. Proposed Secure OFDM-PON

A. Basic Principle

The basic principle of CNOM-based encryption is illustrated in Fig. 1(a). By jointly controlling the original bandwidth of modulated OFDM symbols and their scale factors, the bandwidth of different encrypted OFDM symbols can be maintained at a constant as: $\alpha_i B_{\mathrm{OFDM},i} = \beta$, where i denotes the symbol index, α_i is the i-th scale factor, $B_{\mathrm{OFDM},i}$ is the original bandwidth of the i-th OFDM symbol before encryption, and β is the fixed bandwidth of all encrypted OFDM symbols. It should be noted that the scale factor can be either smaller or greater than 1, depending on the chosen chaotic system and security keys. Without loss of generality, in Fig. 1(a), we only depict the case of α_i<1 for illustrations. In practical applications, the scale factor is determined by the original number (N_i) of subcarriers and a fixed number (M) of subcarriers after encryption, as: $\alpha_i = M / N_i$.

The project was partially supported by a research grant (GRF Project No. 14205820) from the Hong Kong Research Grants Council (Corresponding author: Chun-Kit Chan).

The authors are with the Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong (e-mail: hz016@ie.cuhk.edu.hk; sp020@ie.cuhk.edu.hk; ckchan@ie.cuhk.edu.hk).

Zhouyi Hu is now with Aston Institute of Photonic Technologies, Aston University, Birmingham, B4 7ET, United Kingdom (e-mail: z.hu6@aston.ac.uk).

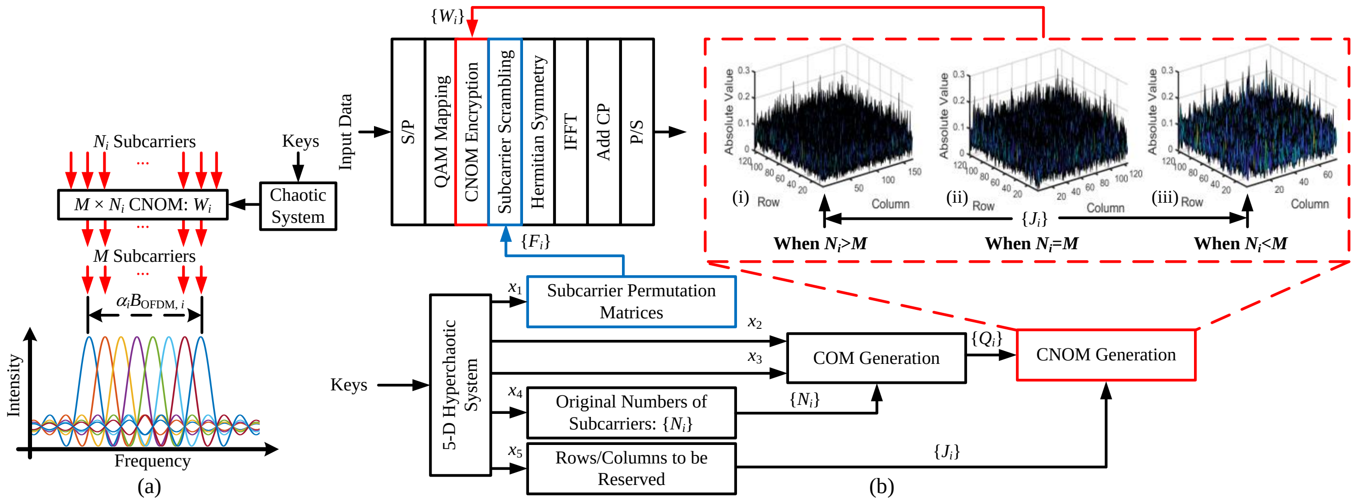

Fig. 1. (a) Principle of CNOM-based encryption. (b) Block diagram of the proposed secure PON based on CNOM encryption, where M=125 for illustration; Insets (i) - (iii): CNOMs $\{W_i\}$ after rows/columns selection according to $\{J_i\}$.

The encryption can then be described as: $X_i = W_i S_i$, where S_i is an N_i×1 vector representing the original data allocated over N_i subcarriers, W_i is an M×N_i CNOM generated by the chaotic system, and X_i is an M×1 vector representing the encrypted data re-allocated over M subcarriers.

The procedure of encryption and decryption is analyzed under three scenarios, according to the value of the scale factor. (1) When α_i<1 (M<N_i), the encryption is equivalent to performing FTN signaling [10]. An additional soft-decision decoder is therefore required at the receiver for inter-carrier interference (ICI) elimination [12], where the corresponding correlation matrix C_i is given by, $C_i = W_i^{\mathrm{H}} W_i$. Here, $(\cdot)^{\mathrm{H}}$ denotes the operation of Hermitian transpose. (2) When α_i=1 (M=N_i), W_i becomes a COM. Therefore, there is no need for any additional soft-decision decoders, and the encryption will not induce any additional penalty. (3) When α_i>1 (M>N_i), the encryption is equivalent to applying redundant precoding [11] to the original signal. The additional soft-decision decoder can also be omitted. Moreover, the system robustness is increased at the expense of SE.

B. Encryption Process

By utilizing CNOMs, we design a secure OFDM-PON, where its transmitter is illustrated in Fig. 1(b). Herein, we adopt a 5-dimensional (5-D) hyperchaotic system [13] to generate the required CNOMs $\{W_i\}$ and the conventional subcarrier permutation matrices $\{F_i\}$ [14]. The state equation of this 5-D hyperchaotic system is described by,

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \\ \dot{x}_5 \end{pmatrix} = \begin{pmatrix} -0.5 & -4.9 & 5.1 & 1 & 1 \\ 4.9 & -5.3 & 0.1 & 1 & 1 \\ -5.1 & 0.1 & 4.7 & 1 & -1 \\ 1 & 2 & -3 & -0.1 & -1 \\ -1 & 1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} + \begin{pmatrix} \varepsilon \sin(\sigma x_2) \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{1}$$

where ε and σ are the parameters controlling the system. In this work, we set ε to 6, and σ to 8.

The detailed encryption process using the 5-D hyperchaotic system described by Eq. (1) is then given as follows,

Step 1: Iterate Eq. (1) by Runge-Kutta 4th-order method to obtain the five chaotic sequences of x_1, x_2, x_3, x_4 and x_5.

Step 2: Generate the subcarrier permutation matrices $\{F_i\}$ from x_1, as,

$$P_i = \mathrm{sort}\left(\mathrm{mod}\left(\left(\left| x_{1,i} \right| - \mathrm{floor}\left(\left| x_{1,i} \right| \right) \right) \times 10^{14}, 256 \right) \right), \tag{2}$$

where $x_{1,i}$ is an M-dimensional vector, which is obtained from the i-th segment of x_1; The function sort(·) indicates the generation of an index vector according to the descending order of the values; P_i is the chaotic permutation vector for generating the corresponding permutation matrix F_i [14]. Since F_i is an orthogonal matrix, the decryption at the receiver side can be readily realized by multiplying its transpose.

Step 3: Generate the COMs $\{Q_i\}$ from the chaotic sequences x_2, x_3, and the original numbers of subcarriers $\{N_i\}$ from x_4. Since every unitary/orthogonal matrix can be expressed as the product of a certain number of complex/real-valued Householder matrices [15], we obtain Q_i as,

$$\begin{aligned} u_{i,k} &= \mathrm{mod}\left(\left(\left| x_{2,i} \right| - \mathrm{floor}\left(\left| x_{2,i} \right| \right) \right) \times 10^{14}, k \right) \\ &\quad + j \cdot \mathrm{mod}\left(\left(\left| x_{3,i} \right| - \mathrm{floor}\left(\left| x_{3,i} \right| \right) \right) \times 10^{14}, k \right), \end{aligned} \tag{3}$$

$$Q_i = \prod_{k=1}^{K} \left(I - 2 \frac{u_{i,k} u_{i,k}^{\mathrm{H}}}{u_{i,k}^{\mathrm{H}} u_{i,k}} \right), \tag{4}$$

where $x_{2,i}$ and $x_{3,i}$ are both N_Q-dimensional vectors obtained from the i-th segment of x_2 and x_3, respectively. Here, we have $N_Q \triangleq \max(N_i, M)$. There are three cases: (1) when N_i>M, the COM Q_i is an N_i×N_i matrix for the FTN signaling; (2) when N_i=M, Q_i is an N_i×N_i (M×M) matrix for the orthogonal precoding; (3) when N_i<M, Q_i is an M×M matrix for the redundant precoding. K denotes the number of iterations, which highly affects the chaotic behavior of COMs [9]. In this work, K was set to

1024 to get decent randomness. Herein, j represents the imaginary unit, and I is an identity matrix with a matching size. Since M is fixed in the proposed encryption, the scale factors $\{\alpha_i\}$ are directly determined by the original numbers of subcarriers $\{N_i\}$, which can be obtained from x_4, as,

$$N_i = \text{floor}\left(\text{mod}\left(\left(\left|x_{4,i}\right| - \text{floor}\left(\left|x_{4,i}\right|\right)\right)\times 10^{14}, D+1\right)\right) + N_{\text{Min}}\ , \quad (5)$$

where $x_{4,i}$ is an element of x_4; D denotes the dynamic range of N_i, determining both the security performance and the transmission performance; N_{Min} is the minimum value of $\{N_i\}$.

Step 4: Determine which rows/columns should be reserved according to x_5 and N_i, as,

$$G_i = \text{sort}\left(\text{mod}\left(\left(\left|x_{5,i}\right| - \text{floor}\left(\left|x_{5,i}\right|\right)\right)\times 10^{14}, 256\right)\right), \quad (6)$$

$$J_i = \begin{cases} G_i\left(1:M\right),\ N_i > M \\ G_i \qquad\quad\ ,\ N_i = M \\ G_i\left(1:N_i\right),\ N_i < M \end{cases}. \quad (7)$$

Similar to Step 3, the dimension of vector $x_{5,i}$ is N_Q. As shown in insets (i)-(iii) of Fig. 1(b), some rows or columns of Q_i are selected according to J_i to generate the corresponding CNOM W_i with a size of $N_i \times M$. The randomness and unpredictability of CNOMs can also be observed from these insets.

C. *Complexity, Security and Transmission Performance*

The complexity of the proposed encryption can be divided into three parts: (1) Iterate the hyperchaotic model in Eq. (1) by Runge-Kutta 4th-order method; (2) Generate CNOMs $\{W\}_i$ and subcarrier permutation matrices $\{F_i\}$ using Eq. (2) - Eq. (7); (3) Perform the encryption ($\{W_i\}$ and $\{F_i\}$) at the system level as shown in Fig. 1(b); However, it should be noted that in practical applications, we do not need to iterate the 5-D hyperchaotic system or update $\{W_i\}$ and $\{F_i\}$ frequently until the security keys have changed at the OLT. In this case, the major computational complexity would only come from the encryption at the system level, i.e., part (3), which totally requires $N_i M$ multiplications, and $\left(N_i - 1\right)M$ additions for each OFDM symbol.

Eavesdroppers can attack the encrypted system by trying to recover either security keys, i.e., the initial condition ($x_1(0)$-$x_5(0)$) and controlling parameters (ε and σ) in this work, or the particular encryption scheme used, i.e., CNOMs in this work. Both can be used for key space calculation. Since herein, we would like to highlight the security performance improved by the newly introduced dimension of non-orthogonality rather than the chaotic model that we chose, only the increase of the key space calculated by the possible combinations of CNOMs was given for a meaningful comparison with our previous work. As we mentioned in Step 3, the dynamic range D of N_i determines both the security performance and the transmission performance. As D increases, the total key space against the exhaustive search attack increases exponentially to $(D+1)^L$, where L is the frame size. It should be noticed that this increase in key space is from the dimension newly provided by the proposed CNOMs and does not exist in the conventional COM-based encryption [9] which follows as a special case of the CNOM-based encryption by setting D=0. However, due to the limitation of FTN signaling, a large D will cause degradation of transmission performance.

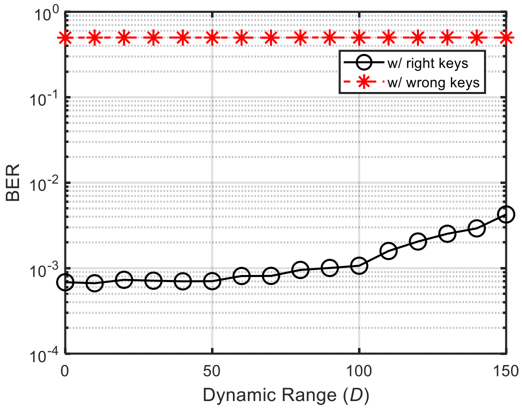

Fig. 2. Impact of dynamic range on the transmission performance.

In Fig. 2, we have investigated the impact of D on the performance of an OFDM signal. For the sake of simplicity in analysis, only an additive white Gaussian noise (AWGN) channel is assumed in this intensity-modulated/direct-detection (IM/DD) OFDM system, where the signal-to-noise ratio (SNR) was set to 10 dB. As shown in the transmitter in Fig. 1(b), a 256-point inverse fast Fourier transform (IFFT) was used for modulation with the additional Hermitian symmetry, and M was therefore set to 125. N_{Min} was set to M–D/2, so the overall SE and data rate can be fixed. Without loss of generality, 4-QAM symbols were used for modulation, and a simple binary-phase-shift-keying iterative detection (CBID) algorithm [12] was employed at the receiver for the soft-decision decoding. We can see from Fig. 2 that the bit-error rate (BER) curve is relatively stable before D is greater than 50, but it starts increasing slightly and significantly when D reaches 50 and 100, respectively. It is because some scale factors (α_{min}=100/125=0.8 and α_{min}=75/125=0.6, respectively) have become too small to fully recover the data. In practical applications, there is a tradeoff between security performance and transmission performance. It should be noticed that the choice of D and the distribution of $\{N_i\}$ can also be used to further enhance the security performance and control the overall data rate.

III. Experimental Demonstration

We then experimentally demonstrated the proposed secure OFDM-PON, as shown in Fig. 3. In this proof-of-concept experiment, M and D were set to 125 and 50, respectively. For a fair comparison, N_{Min} was set to 100, so N_i can be randomly chosen with a uniform distribution over [100, 150]. By doing so, the average number of effectively modulated subcarriers of the encrypted signal with CNOMs was fixed to 125, which was the same as the OFDM signal without encryption or with only orthogonal precoding. Original data were mapped to 4-QAM symbols, and then encrypted by $\{W_i\}$ and $\{F_i\}$. The frame size L was set to 128 in this work, so the number of all possible combinations of $\{W_i\}$ was 3.7×10^{218} ($\approx 51^{128}$). Meanwhile, the

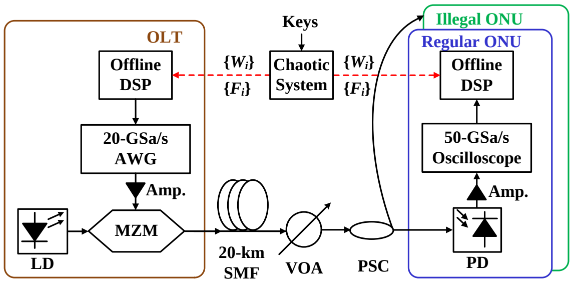

Fig. 3. Proof-of-concept experimental setup for verifying the proposed secure OFDM-PON.

chaotic behavior of CNOMs and the conventional subcarrier scrambling from $\{F_i\}$ can provide additional security enhancement. Due to the Hermitian symmetry for intensity modulation, the size of IFFT was set to 256, where its 1/16 was set as the cyclic prefix (CP). At the OLT, the encrypted data was first sent to an arbitrary waveform generator (AWG) working at 20 GSample/s for digital-to-analog conversion, so the data rate excluding the CP was about 18.4 Gb/s (≈20G×2×125/256×16/17). A Mach-Zehnder modulator (MZM) with a 1550-nm laser diode (LD) then converted the electrical signal after amplification into the optical domain. After transmission over a 20-km single-mode fiber (SMF), a variable optical attenuator (VOA) was employed at the receiver to emulate different received optical power (ROP) values. A power splitter/coupler (PSC) was then used to send the encrypted data to a regular ONU and an illegal ONU simultaneously. After detection by a photodiode (PD), the amplified signal was captured by a 50-GSample/s real-time oscilloscope. Data were finally restored by using right and wrong keys at two ONUs, respectively. It should be noted that a dedicated and secure link is recommended for the key distribution between OLT and ONUs, for instance, using quantum key distribution. Herein, only a tiny difference ($\Delta x_2(0)=1\times10^{-15}$) was induced between the right and the wrong keys.

The experimental results are presented in Fig. 4. Herein, we have also investigated the performance of the COM-based encryption [9] for comparison. We can see from the figure that compared to COM, CNOM only shows a slight penalty at the high ROP region, whereas a new dimension for encryption can provide a huge increase in the key space (about 3.7×10^{218} times in the work) against the exhaustive search attack. Meanwhile, both COM and CNOM outperform the conventional DC-biased optical (DCO-) OFDM signal without encryption, which can be attributed to their coding gain [9]. With a wrong security key, the BER is always 0.5, which means no useful information can be recovered by the illegal ONU.

IV. Summary

In this letter, we have proposed a novel encryption scheme for secure OFDM-PONs. By utilizing CNOMs, the newly introduced dimension for encryption provides a huge increase in the key space. Depending on the chosen 5-D hyperchaotic system and security keys, the encryption performs either FTN signaling or redundant precoding, which can simultaneously improve the security performance and control the overall data rate. Although there is a tradeoff between security performance and transmission performance, the coding gain of the proposed scheme has been verified, via a proof-of-concept experiment. The results indicated the great potential of the proposed CNOM-based encryption in future high-security and high-speed PONs.

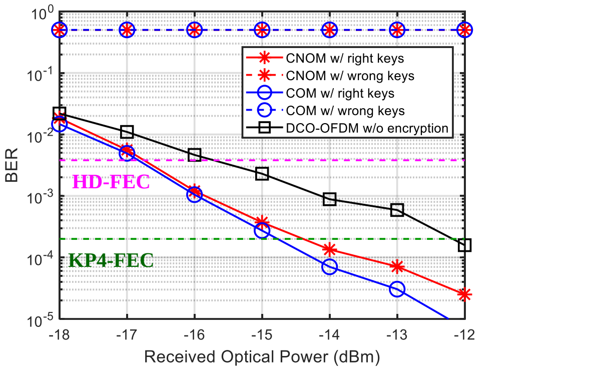

Fig. 4. Measured transmission and security performance of the proposed scheme.

References

[1] N. Cvijetic, "OFDM for next-generation optical access networks," *J. Lightw. Technol.*, vol. 30, no. 4, pp. 384–398, Feb. 15, 2012.

[2] C. W. Chow, C. H. Yeh, C. H. Wang, F. Y. Shih, C. L. Pan, and S. Chi, "WDM extended reach passive optical networks using OFDM-QAM," *Opt. Express*, vol. 16, pp. 12096-12101, 2008.

[3] C. W. Chow, C. H. Yeh, C. H. Wang, C. L. Wu, and C. Lin, "Studies of OFDM signal for broadband optical access networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 6, pp. 800–807, Aug. 2010.

[4] D. Qian, N. Cvijetic, J. Hu, and T. Wang, "108 Gb/s OFDMA-PON with polarization multiplexing and direct detection," *J. Lightw. Technol.*, vol. 28, no. 4, pp. 484–493, Feb. 2010.

[5] A. A. Hajomer, L. Zhang, X. Yang, and W. Hu, "Accelerated key generation and distribution using polarization scrambling in optical fiber," *Opt. Express*, vol. 27, no. 24, pp. 35761–35773, 2019.

[6] Y. Xiao, Y. Chen, C. Long, J. Shi, J. Ma, and J. He, ''A novel hybrid secure method based on DNA encoding encryption and spiral scrambling in chaotic OFDM-PON,'' *IEEE Photon. J.*, vol. 12, no. 3, Jun. 2020, Art. no. 9070154.

[7] T. Wu, C. Zhang, H. Wei, and K. Qiu, "PAPR and security in OFDMPON via optimum block dividing with dynamic key and 2D-LASM," *Opt. Express*, vol. 27, no. 20, pp. 27946–27961, Sep. 2019.

[8] M. Li, B. Liu, R. Ullah, J. Ren, Y. Mao, S. Han, J. Zhao, R. Tang, S. Chen, and J. Ling, "5D data iteration in a multi-wavelength OFDM-PON using the hyperchaotic system". *Optics Letters*, vol. 45, no. 17, 4960-4963, 2020.

[9] Z. Hu and C. K. Chan, ''A real-valued chaotic orthogonal matrix transform-based encryption for OFDM-PON,'' *IEEE Photon. Technol. Lett.*, vol. 30, no. 16, pp. 1455–1458, Aug. 15, 2018.

[10] Z. Hu and C. K. Chan, "Non-orthogonal matrix precoding based faster-than-Nyquist signaling over optical wireless communications," *in Optical Fiber Communication Conference* (Optical Society of America, March 2020), Mar. 2020, Paper. M1J. 5.

[11] S. Ohno and G. B. Giannakis, "Optimal training and redundant precoding for block transmissions with application to wireless OFDM," *IEEE Trans. Commun.*, vol. 50, pp. 2113–2123, Dec. 2002.

[12] J. Huang, Q. Sui, Z. Li, and F. Ji, "Experimental demonstration of 16-QAM DD-SEFDM with cascaded BPSK iterative detection," *IEEE Photon. J.*, vol. 8, no. 3, pp. 1–9, Jun. 2016.

[13] C. Shen, S. Yu, J. Lu, and G. Chen, "A systematic methodology for constructing hyperchaotic systems with multiple positive Lyapunov exponents and circuit implementation," *IEEE Trans. Circuits Syst. I*, Reg. Papers, vol. 61, no. 3, pp. 854–864, Mar. 2014.

[14] Z. Hu and C. K. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON," *J. Lightwave Technol.*, Vol. 36, no. 16, pp. 3373–3381, 2018.

[15] G. Golub, C. Van Loan, *Matrix Computations*, second ed., Johns Hopkins University Press, Baltimore, 1989, Chapters 5.1, 5.2.