JOURNAL OF
Optical Communications
and Networking

Multi-band chaotic non-orthogonal matrix-based encryption for physical-layer security enhancement in OFDM-PONs

PEIJI SONG,[1] ZHOUYI HU,[2,3,*] AND CHUN-KIT CHAN[1]

[1]Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong, China
[2]Aston Institute of Photonic Technologies, Aston University, Birmingham B4 7ET, UK
[3]Now with Department of Electrical Engineering, Eindhoven University of Technology, 5600 MB Eindhoven, The Netherlands
*z.hu@tue.nl

Received 15 November 2022; revised 23 February 2023; accepted 3 March 2023; published 2 June 2023

In this paper, we propose and experimentally demonstrate a novel multi-band chaotic non-orthogonal matrix (CNOM)-based encryption scheme for secure orthogonal frequency division multiplexing (OFDM) passive optical networks. The dimension of non-orthogonality is exploited in the encryption with the CNOM, where both faster-than-Nyquist signaling and redundant precoding were employed to dynamically scramble the original number of subcarriers of each sub-band and fix the overall data rate. Both simulation and experimental results of a 10.6 Gb/s 4-QAM transmission over a 20-km standard single-mode fiber showed that the total key space significantly increases by 1.4×10^{482} and 1.72×10^{653} times, as the number of sub-bands increases from 1 to 10 and 15, with a considerable reduction in computational complexity of 90% and 93.33% in complex-valued multiplication, and 90.76% and 94.12% in complex-valued addition, when encrypting one OFDM symbol, respectively. Moreover, the improved resilience to the frequency roll-off has also been verified by using additional permutation matrices in the proposed encryption algorithm.

https://doi.org/10.1364/JOCN.481071

1. INTRODUCTION

With advantages such as low power consumption, large capacity, and easy maintenance, the passive optical network (PON) has been widely deployed over the past few decades. It is well-recognized as a promising solution to solve the "last mile" bottleneck of the access network. On the other hand, orthogonal frequency division multiplexing (OFDM) has been extensively investigated in PONs owing to its high spectral efficiency (SE), high robustness against channel chromatic dispersion, and high flexibility [1]. Therefore, OFDM-PONs have drawn extensive attention from academia and industry [2–4]. Nonetheless, most previous studies on OFDM-PONs mainly focused on achieving optimal transmission performance rather than their security issues. Communication security is increasingly crucial, with massive PONs deployed for financial and government business use. In conventional OFDM-PONs, the optical line terminal (OLT) uses a broadcasting method to transmit downstream data to all optical network units (ONUs), making the transmitted data very susceptible to illegal eavesdropping. To cope with this challenge, improving the security performance in OFDM-PONs has become a hot research area [5–7].

Although different types of encryption methods have been proposed, many of them mainly focused on the high-level encryption protocol of the network, such as employing cryptographic protocols at the media access control layer [8,9]. With the advent of the quantum computing era, those aforementioned methods are at risk of being cracked within a short period of time. By contrast, encryption at the physical layer can take the security performance to a higher level and is more suitable for high-speed data encryption than high-level encryption [10–12].

Chaos-based encryption, such as optical chaos encryption using feedback lasers and digital chaos encryption with nonlinear differential equations, is a potential solution for physical-layer security enhancement due to its high sensitivity to initial values, high randomness, large bandwidth, and low latency [13,14]. Nevertheless, the optical chaos encryption based on feedback lasers imposes high cost and complexity on the system, which can be avoided by replacing it with digital chaos encryption without additional hardware utilization. There have been a variety of encryption schemes based on digital chaos proposed in recent years, such as DNA and chaos coding [15], Brownian motion and chaos [16], constellation disruption [17], and phase masking and frequency-time confusion [18]. However, in many aforementioned techniques, only the primitive permutations are generally used for scrambling, leading to high complexity, time delay, and synchronization

errors. In our previous work, by introducing a new dimension of non-orthogonality for encryption, we have proposed a single-band chaotic non-orthogonal matrix (CNOM)-based encryption algorithm [12] that can achieve a higher key space compared to the chaotic orthogonal matrix (COM)-based encryption reported in [10]. Nonetheless, only the case of one sub-band encryption has been studied.

At ECOC 2022, we propose a novel multi-band CNOM-based encryption scheme by generalizing the concept of single-band CNOM-based encryption to a more common case for further enhancement of the physical-layer security in OFDM-PONs [19]. In this paper, we extend our work by analyzing the encryption complexity in more detail and giving more comprehensive results and discussions about how the key space, computational complexity, and transmission performance change with the number of sub-bands, which is important to guide how to choose the appropriate number of sub-bands in practical application. In the proposed encryption scheme, the whole bandwidth of the OFDM symbols is first divided into L sub-bands. Then, for each sub-band, a set of independent CNOMs is used for encryption, which is determined by a five-dimensional (5-D) hyperchaotic system and the corresponding preoptimized dynamic range (D_L) of the original number of subcarriers. The dimension of non-orthogonality is employed in encryption with CNOMs, where both faster-than-Nyquist (FTN) signaling [20] and redundant precoding [21] are utilized to increase the key space and fix the overall data rate. Moreover, we investigate the impact of the number of sub-bands L and the corresponding dynamic range D_L in encryption on transmission performance, security performance, and computational complexity. Finally, the encrypted signal with a 10.6-Gb/s data rate using the 4-QAM modulation format was successfully transmitted over a 20-km standard single-mode fiber (SSMF). The experimental results show that by employing the proposed multi-band encryption scheme with the optimal dynamic range, an enormous increase in the key space and a decrease in computational complexity can be realized at the cost of a moderate penalty in the transmission performance, providing increased flexibility of encryption in practical applications. Specifically, when the number of sub-bands increases from 1 to 10 and 15, the key space can increase by 1.4×10^{482} and 1.72×10^{653} times, respectively. Meanwhile, the complexity can be reduced by 90% and 93.33% in complex-valued multiplication, and 90.76% and 94.12% in complex-valued addition, when encrypting one OFDM symbol, respectively. Finally, the experimental results confirm that additional permutation matrices used for scrambling the encrypted subcarriers in this work can also increase the tolerance to the frequency roll-off of a communication system.

The rest of the paper is organized as follows: Section 2 describes the proposed multi-band CNOM-based encryption scheme in detail. The experimental setup and corresponding digital signal processing (DSP) are given in Section 3. Section 4 presents the experimental results and the discussion. Finally, Section 5 summarizes this paper.

2. PROPOSED SECURE OFDM-PON

A. Multi-band CNOM-Based Encryption

Figure 1 shows the basic principle of the multi-band CNOM-based encryption. First, the overall bandwidth of the OFDM symbols is divided into L sub-bands evenly. Then, independent CNOMs are applied to these sub-bands for encryption. In Fig. 1, we use the lth sub-band of the kth OFDM symbol as an example for illustration. It should be noted that the bandwidth of each sub-band after encryption in all OFDM symbols is set to the same value to facilitate the operation in this work. Herein, the bandwidth of the lth encrypted sub-band can be set to $\beta = \alpha_{lk} B_{lk}$, where α_{lk} is the scale factor applied to the lth sub-band of the kth OFDM symbol, and B_{lk} is the corresponding original bandwidth. We can thus fix the value of β by jointly controlling α_{lk} and B_{lk}. For the CNOM-based encryption of the lth sub-band, the scale factor α_{lk} can be either greater or smaller than 1, depending on the chosen chaotic system and the corresponding security key. Figure 1 illustrates all three cases of $\alpha_{lk} < 1$, $\alpha_{lk} > 1$, and $\alpha_{lk} = 1$. In our designed system, the scale factor α_{lk} is obtained by $\alpha_{lk} = M/N_{lk}$, where N_{lk} is the original number of subcarriers determined by the chaotic system, which is related to the original bandwidth B_{lk}, and M is the fixed number of subcarriers for the lth sub-band after encryption, which is related to β. M is derived from $M = V/L$, where V denotes the total number of subcarriers after encryption, and V is also fixed during the encryption process.

The mathematical representation of encryption for the lth sub-band of the kth OFDM symbol can be described as $\boldsymbol{X_{lk}} = \boldsymbol{W_{lk}} \boldsymbol{S_{lk}}$, where $\boldsymbol{S_{lk}}$ is an $N_{lk} \times 1$ vector that represents the original data loaded over N_{lk} subcarriers of the lth sub-band, $\boldsymbol{W_{lk}}$ is an $M \times N_{lk}$ chaotic matrix generated by the chaotic system, and $\boldsymbol{X_{lk}}$ is an $M \times 1$ vector representing the encrypted data reallocated over M subcarriers. Then, the encrypted subcarriers of total L sub-bands are scrambled by another permutation matrix $\boldsymbol{F_k}$ with a size of $V \times V$, which is also generated by the chaotic system and is different for different OFDM symbols.

Based on the value of the scale factor α_{lk}, we can classify the encryption and decryption for the lth sub-band of the kth OFDM symbol into three cases. (1) When $\alpha_{lk} < 1$, $\boldsymbol{W_{lk}}$ is a CNOM. In this case, the encryption is equivalent to performing FTN signaling [20], purposely inducing inter-carrier interference (ICI) that needs to be eliminated by an additional soft-decision decoder at the receiver side [22].

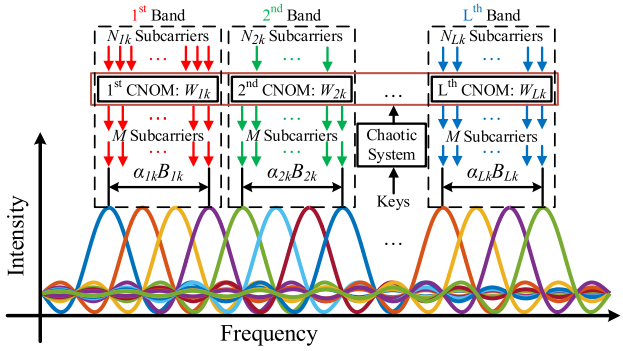

Fig. 1. Principle of multi-band CNOM-based encryption.

(2) When $\alpha_{lk}=1$, $\boldsymbol{W_{lk}}$ becomes a COM [10]. In this case, the encryption does not introduce any penalty, thus without requiring additional soft-decision decoders. (3) When $\alpha_{lk}>1$, the encryption becomes redundant precoding [21]. Therefore, an extra soft-decision decoder is also not needed in this case. Meanwhile, the system's robustness can be improved at the expense of SE.

B. Encryption Process

Based on the encryption principle described above, Fig. 2 shows the transmitter DSP of our designed secure OFDM-PONs. Here, we use a 5-D hyperchaotic system to generate the required chaotic precoding matrices $\{\boldsymbol{W_{lk}}\}$ and the subcarrier permutation matrices $\{\boldsymbol{F_k}\}$ [11]. It should be noted that the subcarrier permutation matrices $\{\boldsymbol{F_k}\}$ used in [11] are set to be the same for all OFDM symbols. In this work, $\{\boldsymbol{F_k}\}$ are varied for different OFDM symbols to achieve a coding gain and improved security performance. The state equation of this 5-D hyperchaotic system is given by [23]

$$\begin{pmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\\ \dot{x}_5\end{pmatrix}=\begin{pmatrix}-0.5 & -1.9 & 5.1 & 1 & 1\\ 4.9 & -5.3 & 0.1 & 1 & 1\\ -5.1 & 0.1 & 4.7 & 1 & -1\\ 1 & 2 & -3 & -0.1 & -1\\ -1 & 1 & 1 & 1 & -1\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\\ x_4\\ x_5\end{pmatrix}+\begin{pmatrix}\varepsilon\sin(\sigma x_2)\\ 0\\ 0\\ 0\\ 0\end{pmatrix}, \tag{1}$$

where ε and σ are the parameters that control the system, and their values are set to 6 and 8, respectively, in this work.

The detailed encryption process using Eq. (1) as the hyperchaotic system is then given as follows:

Step 1: Iterate Eq. (1) by the Runge–Kutta fourth-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 $\{\boldsymbol{F_k}\}$ from x_1 as

$$P_k=\mathrm{sort}(\mathrm{mod}((|x_{1,k}|-\mathrm{floor}(|x_{1,k}|))\times 10^{14},256)), \tag{2}$$

where $x_{1,k}$ is a V-dimensional vector, which corresponds to the kth segment of x_1. The function sort$(\cdot)$ represents the generation of an index vector in descending order of the input values. P_k is the generated chaotic permutation vector, which is then used to get the permutation matrix $\boldsymbol{F_k}$. Since $\boldsymbol{F_k}$ is orthogonal, we can easily realize its associated decryption process by multiplying its transpose at the receiver side.

Step 3: Generate the COMs $\{\boldsymbol{Q_{lk}}\}$ from the chaotic sequences x_2 and x_3, and acquire the corresponding original numbers of subcarriers $\{N_{lk}\}$ from x_4. Utilizing the property that every unitary matrix can be expressed as the product of a certain number of Householder matrices [24], we obtain $\boldsymbol{Q_{lk}}$ as

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

$$\boldsymbol{Q_{lk}}=\prod_{b=1}^{B}\left(\boldsymbol{I}-2\frac{u_{l,k,b}u_{l,k,b}^{H}}{u_{l,k,b}^{H}u_{l,k,b}}\right), \tag{4}$$

where $x_{2,l,k}$ and $x_{3,l,k}$ are vectors with the same length of $N_{Q,l,k}$ $(N_{Q,l,k}=\max(N_{lk},M))$ obtained from the $(L\times k+l)$th segment of x_2 and x_3, respectively; $(\cdot)^H$ represents the operation of conjugate transpose; b denotes the bth iteration; and B is the total number of iterations in generating $\boldsymbol{Q_{lk}}$, which highly affects the chaotic behavior of COMs [10]. To guarantee decent randomness, B is set to 1024 in this work. As shown in insets (i)–(iii) of Fig. 2, the precoding is classified into three scenarios: (1) when $N_{lk}>M$, the COM $\boldsymbol{Q_{lk}}$ is an $N_{lk}\times N_{lk}$ matrix, where some rows will be discarded during encryption to perform the FTN signaling; (2) when $N_{lk}=M$, $\boldsymbol{Q_{lk}}$ is an $N_{lk}\times N_{lk}$ or $M\times M$ matrix for the orthogonal precoding; and (3) when $N_{lk}<M$, $\boldsymbol{Q_{lk}}$ is an $M\times M$ matrix, where some columns will be discarded during encryption to perform the redundant precoding. Besides, j is the imaginary unit, and $\boldsymbol{I}$ denotes an identity matrix with a corresponding size. Since M is fixed for all sub-bands, the scale factors $\{\alpha_{lk}\}$

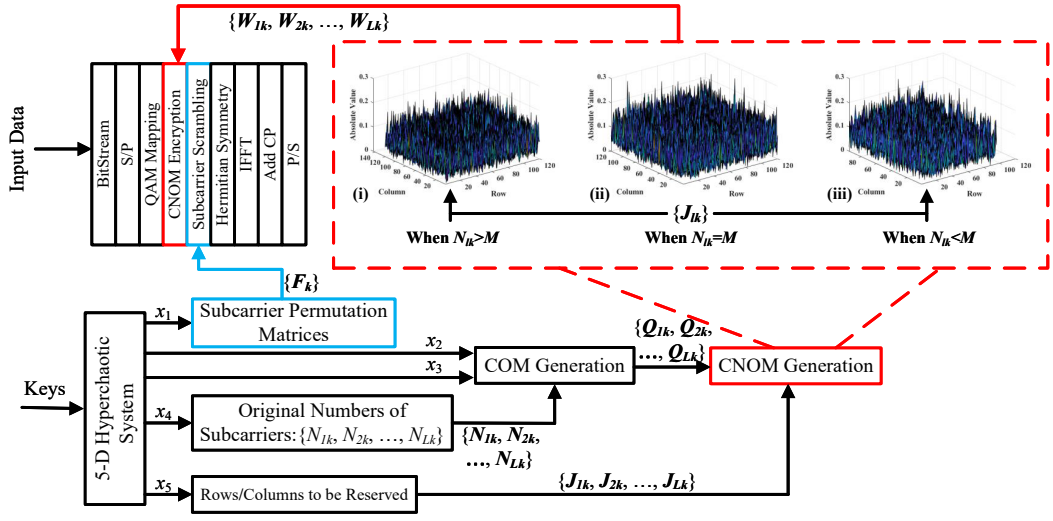

Fig. 2. Block diagram of the proposed secure OFDM-PONs based on multi-band CNOM encryption. Insets (i)–(iii): CNOMs $\boldsymbol{W_{lk}}$ after selection of rows/columns according to $\boldsymbol{J_{lk}}$.

are only determined by the original numbers of subcarriers $\{N_{lk}\}$. N_{lk} is obtained from x_4 as

$$N_{lk} = \text{floor}(\text{mod}((|x_{4,l,k}| - \text{floor}(|x_{4,l,k}|)) \times 10^{14}, D_L + 1) + N_{L,\text{Min}}, \tag{5}$$

where D_L represents the dynamic range of N_{lk}, determining both the security and transmission performance. Generally speaking, for a fixed L, a larger D_L corresponds to a larger key space. However, it leads to transmission performance degradation when D_L has increased to a certain proportion of M due to the influence of FTN precoding [12]. Since M is related to L, the optimal D_L is also related to L. Besides, the computational complexity of the encryption process is also dependent on L shown in Subsection 2.C. $N_{L,\text{Min}}$, which is obtained by $N_{L,\text{Min}} = M - D_L/2$, is the minimum value of N_{lk}.

Step 4: Determine the rows/columns $\{\boldsymbol{J_{lk}}\}$ that should be reserved according to x_5 and N_{lk} as

$$\boldsymbol{G_{lk}} = \text{sort}(\text{mod}((|x_{5,l,k}| - \text{floor}(|x_{5,l,k}|)) \times 10^{14}, 256)), \tag{6}$$

$$\boldsymbol{J_{lk}} = \begin{cases} \boldsymbol{G_{lk}}(1:M), & N_{lk} > M \\ \boldsymbol{G_{lk}}, & N_{lk} = M \\ \boldsymbol{G_{lk}}(1:N_{lk}), & N_{lk} < M \end{cases}, \tag{7}$$

where $x_{5,l,k}$ is the $(L \times k + l)$th segment of x_5 with a length of $N_{Q,l,k}$. $\boldsymbol{G_{lk}}$ is an index vector containing the column or row index of the generated $\{\boldsymbol{Q_{lk}}\}$. As shown in insets (i)–(iii) of Fig. 2, we discard some rows or columns of $\boldsymbol{Q_{lk}}$ according to $\boldsymbol{J_{lk}}$ that only contains partial column or row indices of $\boldsymbol{Q_{lk}}$. Specifically, we will discard some rows of $\boldsymbol{Q_{lk}}$ when $N_{lk} > M$, or some columns of $\boldsymbol{Q_{lk}}$ when $N_{lk} < M$, to generate the required chaotic precoding matrix, i.e., the $\boldsymbol{W_{lk}}$ of the CNOM for the lth sub-band of the kth OFDM symbol with a size of $N_{lk} \times M$.

C. Complexity and Key Space Analysis

Then, we evaluate the computational complexity of the proposed multi-band CNOM-based encryption scheme. The complexity can be mainly divided into three parts: (1) iterating Eq. (1) using the Runge–Kutta fourth-order method, (2) generating CNOMs $\{\boldsymbol{W_{lk}}\}$ and subcarrier permutation matrices $\{\boldsymbol{F_k}\}$ using Eqs. (2)–(7), and (3) implementing the encryption ($\{\boldsymbol{W_{lk}}\}$ and $\{\boldsymbol{F_k}\}$) as shown in Fig. 2. The detailed computational complexity analysis step by step is given as follows.

1. Chaotic Model

Step 1: We need to iterate the state equation in Eq. (1) by the Runge–Kutta fourth-order method, where each iteration requires 191 multiplications, 194 additions, and 4 $\sin(\cdot)$ operators. It should be noted that the number of iterations of the Runge–Kutta fourth-order method is predefined by the network operator.

2. Generation of CNOMs $\{\boldsymbol{W_{lk}}\}$ and Subcarrier Permutation Matrices $\{\boldsymbol{F_k}\}$

Step 2: Since $x_{1,k}$ is an M-dimension vector, Eq. (2) requires M multiplications, M additions, M floor$(\cdot)$ operators, M mod$(\cdot)$ operators, $2M$ $|\cdot|$ operators, and 1 sort$(\cdot)$ operator for sorting M elements.

Step 3: Note that both $x_{2,l,k}$ and $x_{3,l,k}$ are vectors with a size of $N_{Q,l,k}$, and Eq. (3) should be performed B times for generating a COM. Therefore, Eq. (3) requires $3N_{Q,l,k}B$ multiplications, $3N_{Q,l,k}B$ additions, $2N_{Q,l,k}B$ floor$(\cdot)$ operators, $2N_{Q,l,k}B$ mod$(\cdot)$ operators, and $4N_{Q,l,k}B$ $|\cdot|$ operators. Meanwhile, Eq. (4) requires $(N_{Q,l,k}^2 + N_{Q,l,k} + 1)B + N_{Q,l,k}^3(B-1)$ multiplications, and $(N_{Q,l,k}^2 + N_{Q,l,k} - 1)B + N_{Q,l,k}^2(N_{Q,l,k} - 1)(B-1)$ additions. Since $(D_L + 1)$ is a frame-level calculation that can be easily obtained by a look-up table, Eq. (5) requires one multiplication, two additions, two floor$(\cdot)$ operators, one mod$(\cdot)$ operator, and two $|\cdot|$ operators.

Step 4: Because $x_{5,l,k}$ is an $N_{Q,l,k}$-dimension vector, Eq. (6) requires $N_{Q,l,k}$ multiplications, $N_{Q,l,k}$ additions, $N_{Q,l,k}$ floor$(\cdot)$ operators, $N_{Q,l,k}$ mod$(\cdot)$ operators, $2N_{Q,l,k}$ $|\cdot|$ operators, and one sort$(\cdot)$ operator for sorting $N_{Q,l,k}$ elements. Equation (7) requires one comparison operator, whose complexity equals that of one addition.

3. Encryption at the System Level

Since the subcarrier permutation matrix $\boldsymbol{F_k}$ with a size of $V \times V$ only has one entry in each row and each column and zeros elsewhere, it does not introduce any computational complexity of multiplications or additions. Meanwhile, the CNOM applied to the lth sub-band has a size of $M \times N_{lk}$. Therefore, the encryption at the system level for L sub-bands requires $\sum_{l=1}^{l=L} N_{lk}M$ multiplications and $\sum_{l=1}^{l=L}(N_{lk} - 1)M$ additions for each OFDM symbol.

The complexity of each part is summarized in Table 1. However, it should be noted that in practical applications, we do not need to iterate Eq. (1) or update $\{\boldsymbol{W_{lk}}\}$ and $\{\boldsymbol{F_k}\}$ frequently until the security keys have changed at the OLT. Therefore, the major computational complexity would only come from the encryption at the system level, i.e., part (3), which is evaluated in the following part.

Since $N_{l,k}$ in Eq. (5) follows the uniform distribution with a mean of M, the expectation of the number of complex-valued multiplications and complex-valued additions of part (3) can be written as

$$\text{Complex-Valued Multiplication} = V^2/L, \tag{8}$$

$$\text{Complex-Valued Addition} = V^2/L - V, \tag{9}$$

respectively, for each encrypted OFDM symbol.

We take $V = 120$ for the following simulation and experiment. Based on Eqs. (8) and (9), as the number of sub-bands L increases from 1 to 10 and 15, the complexity of complex-valued multiplication can be reduced by 90% and 93.33%, respectively. Meanwhile, the complexity of complex-valued addition can be reduced by 90.76% and 94.12%, respectively, when encrypting one OFDM symbol.

Table 1. Computational Complexity of Encryption in Each OFDM Symbol

	Part (1)	Part (2)	Part (3)
Complex-valued multiplication	191	$\left(\sum_{l=1}^{l=L}((N_{Q,l,k}^2+4N_{Q,l,k}+1)B+N_{Q,l,k}^3(B-1)+N_{Q,l,k})\right)+M+L$	$\sum_{l=1}^{l=L}N_{lk}M$
Complex-valued addition	194	$\left(\sum_{l=1}^{l=L}((N_{Q,l,k}^2+4N_{Q,l,k}-1)B+(N_{Q,l,k}^3-N_{Q,l,k}^2)(B-1)+N_{Q,l,k})\right)+M+2L$	$\sum_{l=1}^{l=L}(N_{lk}-1)M$
$\sin(\cdot)$	4	0	0
floor$(\cdot)$	0	$\left(\sum_{l=1}^{l=L}(B+1)N_{Q,l,k}\right)+M+2L$	0
mod$(\cdot)$	0	$\left(\sum_{l=1}^{l=L}(B+1)N_{Q,l,k}\right)+M+L$	0
$\lvert\cdot\rvert$	0	$\left(\sum_{l=1}^{l=L}2(B+1)N_{Q,l,k}\right)+2M+2L$	0
sort$(\cdot)$	0	$1+L$	0

The key space can be calculated by either the sensitivity to the initial value of the security keys [25] or the number of all possible combinations of the matrices used for encryption [26]. Since we would like to emphasize the security performance improved by the proposed multi-band CNOM-based encryption scheme, we have evaluated the security performance by calculating the total number of possible combinations using multi-band CNOMs, facilitating a meaningful comparison with the COM-based encryption and the single-band CNOM-based encryption studied in our previous works [10,12]. As we mentioned in Step 3 in Subsection 2.B, the dynamic range D_L determines the security and the transmission performance for a fixed value of L. Specifically, a larger D_L produces a higher key space but induces a larger transmission performance penalty. Compared with $D_L=0$, i.e., the conventional COM-based encryption, the increase in key space against the exhaustive search attack using the proposed multi-band encryption scheme is given by

$$\xi=((D_L+1)^L)^P, \tag{10}$$

where P is the frame size of OFDM symbols. It should be noted that the single-band CNOM-based encryption in [12] follows as a special case by setting $L=1$. Based on Eqs. (8) and (9), we know that the computational complexity decreases with the increase of L. However, ξ cannot keep increasing because the optimal D_L depends on the value of L. Moreover, the transmission performance will degrade when L is larger than 1 or D_L increases to a certain proportion of M. Therefore, we have also studied the impact of L and the dynamic range D_L on the total size of the key space and transmission performance in Subsection 2.D. For a fair comparison, the total number (V) of subcarriers after encryption has been fixed.

D. Impact of L and D_L on the Transmission Performance and Key Space

In this subsection, we have studied the impact of D_L on the transmission performance of the encrypted intensity-modulated/direct-detection OFDM signals for some representative values of L via numerical simulation. Considering the flexibility and ease of operation in practical applications, the set $\boldsymbol{O}$ containing these representative L was chosen as $\{1, 2, 3, 4, 5, 6, 8, 10, 12, 15\}$ for a fixed $V=120$. For simplicity of analysis, an additive white Gaussian noise channel was assumed in the simulation. Without loss of generality, 4-QAM was used as the modulation format, and the common cascaded binary-phase-shift-keying iterative detection (CBID) algorithm [22] was employed as the soft-decision decoder at the receiver side. It should be noted that the DSP and the signal parameters used in the simulation were the same as those in our experiment to be discussed in Section 3, where the sizes of the inverse fast Fourier transform (IFFT), V and P, were set to 256, 120, and 128, respectively.

We first set the signal-to-noise ratio (SNR) to 10 dB and take $L=1$ as an example, where the corresponding value of M is relatively large. We can see from Fig. 3(a) that the bit error rate (BER) curve is relatively stable until D_1 (i.e., D_L, when $L=1$) is larger than 50. Meanwhile, the BER increases slightly from $D_1=50$ and significantly from $D_1=80$, respectively, which can be attributed to the influence of ICI induced by FTN precoding. The minimum scale factor $\alpha_{\min}$ is 0.83 for $D_1=50$ and 0.75 for $D_1=80$, respectively. The ICI associated with the former is relatively small for easy elimination, but it increases and becomes too large to be easily eliminated for the latter. However, for a large L value, the corresponding value of M becomes relatively small, leading to strong compression effects even with a small D_L, e.g., $D_L=2$. The resultant ICI, therefore, becomes too large to be easily eliminated as shown in Fig. 3(b). Thus, in this work, to maintain a relatively large key space while maintaining a good transmission performance, the optimal D_L was decided by a critical value where the BER is relatively stable for D_L less than or equal to it, and the BER starts increasing slightly for D_L larger than it. Particularly, we can see from Fig. 3(b) that the optimal D_L was set to 2 for the case of $L\geq 8$ because the BER increased even with $D_L=2$. Note that in practical applications, a threshold of the BER penalty (e.g., 10%) caused by L-band encryption can be set for the decision of the optimal D_L. This threshold is dependent on the requirements for the key space, complexity, and transmission performance. Based on this criterion, we have summarized the optimal D_L for all L chosen from set $\boldsymbol{O}$ in Table 2 along with the increase of the key space compared to the COM-based

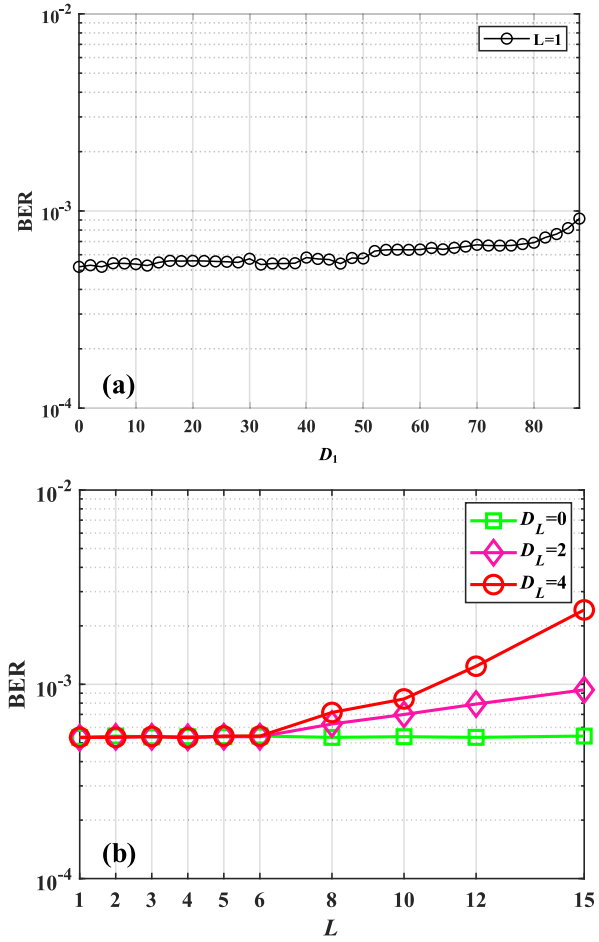

Fig. 3. Simulated results of (a) impact of dynamic range D_1 on the transmission performance for $L = 1$ and (b) BER versus sub-band number L with $D_L = 0$, 2, and 4, where the SNR was set to 10 dB.

Table 2. Optimal D_L for Different L, Along with the Increase of the Key Space

L	Optimal D_L	Key Space
1	50	$51^P = 51^P$
2	16	$(17^2)^P = (289)^P$
3	14	$(15^3)^P = (3375)^P$
4	12	$(13^4)^P = (28{,}561)^P$
5	6	$(7^5)^P = (16{,}807)^P$
6	4	$(5^6)^P = (15{,}625)^P$
8	2	$(3^8)^P = (6561)^P$
10	2	$(3^{10})^P = (59{,}049)^P$
12	2	$(3^{12})^P = (531{,}441)^P$
15	2	$(3^{15})^P = (1.43 \times 10^7)^P$

encryption. Without loss of generality, the optimal D_L for each value of L, as listed in Table 2, was adopted for the following simulations and experiments.

By applying the optimal D_L to the multi-band encryption, we present the relationship between the BER and L in Fig. 4, where the results of a bandwidth-limited channel due to devices and fiber dispersion are also given as the benchmark. The bandwidth-limited channel is emulated by a first-order Bessel filter with a 6-GHz cut-off frequency. In both channels,

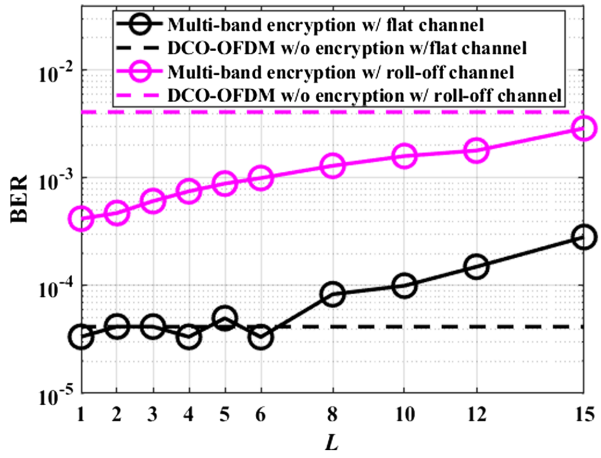

Fig. 4. Simulated BER performance versus the sub-band number using a flat channel, and a roll-off channel realized by a 6-GHz first-order Bessel filter, respectively, where the optimal D_L was applied, and the SNR was set to 11.5 dB for both cases.

the SNR was fixed at 11.5 dB for a fair comparison. It can be observed from Fig. 4 that under a flat channel, the BER is relatively stable and comparable to that of the DC-biased optical (DCO-) OFDM signal without encryption when L is small ($L \leq 6$) and increases as L further increases. This is due to the fact that the influence of ICI can be well eliminated when L is small ($L \leq 6$) and cannot be completely mitigated when L is large ($L > 6$), as shown in Fig. 3(b). Meanwhile, the BER increases significantly under the bandwidth-limited channel, indicating an increased penalty induced by the multi-band structure in this scenario.

3. EXPERIMENTAL SETUP

Figure 5 shows the schematic diagram of this experimental setup, and Fig. 2 gives the transmitter side DSP, whose inverse process is used to demodulate the signal at the receiver side. Initial binary bits after serial to parallel conversion were first mapped into 4-QAM symbols. The whole bandwidth was then divided into L sub-bands before being encrypted with $\{\boldsymbol{W_{lk}}\}$ and $\{\boldsymbol{F_k}\}$, where V and P were set to 120 and 128, respectively, in this experiment. After Hermitian symmetry for intensity modulation, the IFFT with a size of 256 was used to generate a real-valued OFDM signal, where its 1/16 was set as the cyclic prefix (CP). At the OLT, the generated real-valued digital signal after parallel to serial conversion was transformed into an analog signal by an arbitrary waveform generator (AWG) working at 12 Gsample/s. As a result, the data rate excluding the CP was approximately 10.6 Gb/s (= 12 Gb/s × 2 × 120/256 × 16/17. The analog signal was then amplified by an electrical amplifier (EA). A Mach–Zehnder modulator (MZM), together with a laser diode (LD) set to 1550 nm, converted the electrical signal into the optical domain before being fed into a 20-km SSMF link for transmission. At the receiver side, a variable optical attenuator (VOA) was employed to adjust the value of the received optical power (ROP) to measure the sensitivity curve. The encrypted signal was sent to a regular ONU and an illegal ONU via a 50:50 power splitter/coupler (PSC). After detection by a photodiode (PD), the received

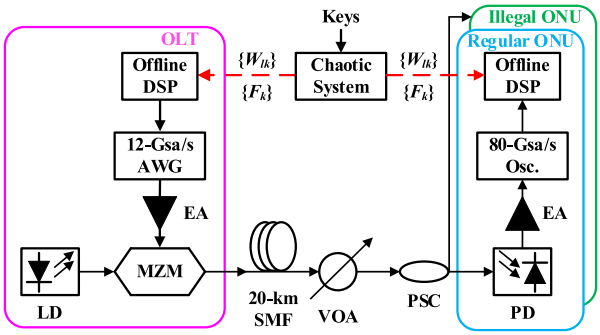

Fig. 5. Proof-of-concept experimental setup for verifying the proposed secure OFDM-PON (LD, laser diode; AWG, arbitrary waveform generator; EA, electrical amplifier; MZM, Mach–Zehnder modulator; SSMF, standard single-mode fiber; VOA, variable optical attenuator; PSC, power splitter/coupler; PD, photodiode).

signal was amplified by another EA and then captured by an 80-Gsample/s real-time oscilloscope. Finally, the detected data after synchronization and equalization was decrypted using the inverse encryption process shown in Fig. 2 with right and wrong keys at two ONUs, respectively.

4. EXPERIMENTAL RESULTS AND DISCUSSION

We first experimentally investigated the impact of different L with the corresponding optimal D_L on the system performance. Figure 6(a) shows the BER versus the value of L, where the ROP was set to -12.5 dBm. We can see from Fig. 6(a) that the BER increases as L increases due to the multi-band structure, corresponding to the results in Fig. 4. Though $L = 1$ corresponds to the best transmission performance, encryption with a larger L can achieve a larger key space and lower computational complexity at the encryption level. Thus, we need to choose an appropriate L by overall considering the requirements of the key space, computational complexity, and transmission performance in a practical system.

Since the BER difference among $L = 1$, 10, and 15 is relatively large, as shown in Fig. 6(a), we have then studied the transmission performance of the proposed multi-band CNOM-based encryption scheme with these three L values. Figure 6(b) presents the BER curves and constellation diagrams under regular reception and illegal reception, where we only made a tiny difference in the security keys ($\Delta x_2 = 10^{-15}$). Herein, the 10 sub-band COM-based encryption was used as the benchmark for comparison. We can see from Fig. 6(b) that, compared to the 10 sub-band COM-based encryption, L sub-band CNOM-based encryption with the right keys shows little performance penalty. In contrast, it can significantly increase the key space by 1.4×10^{482} and 1.72×10^{653} times for $L = 10$ and $L = 15$, respectively, against the exhaustive search attack. Besides, as we mentioned before, as the number of sub-bands increases from 1 to 10 and 15, the complexity of complex-valued multiplication can be reduced by 90% and 93.33%, and the complexity of complex-valued addition can be reduced by 90.76% and 94.12% when encrypting one OFDM symbol. Moreover, it can be observed from Fig. 6(b) that both COM- and CNOM-based encryption outperform the conventional DCO-OFDM signal without encryption.

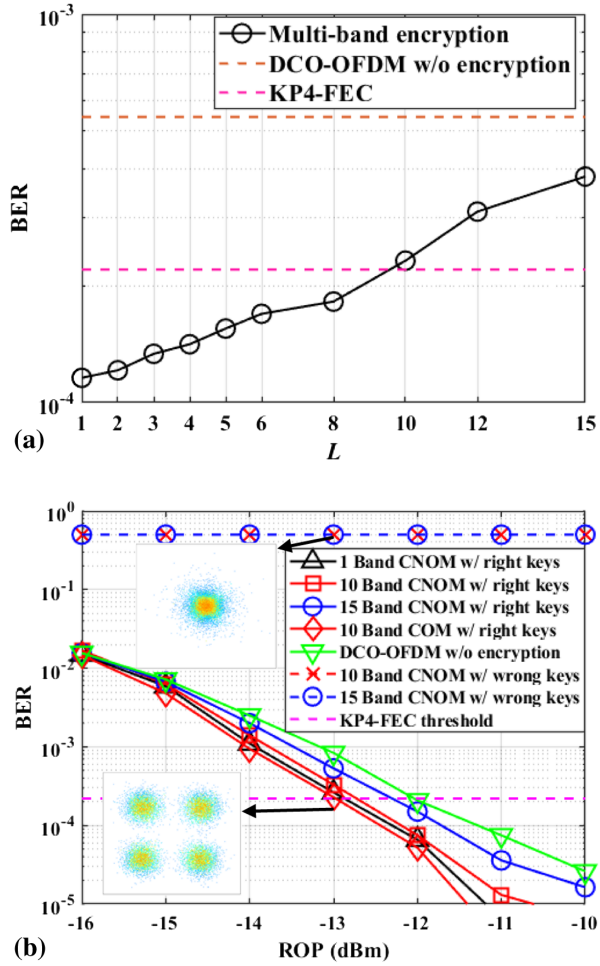

Fig. 6. (a) Measured BER versus sub-band number with ROP $= -12.5$ dBm after 20-km SSMF transmission. (b) BER and the corresponding constellation diagrams of the proposed multi-band CNOM-based encryption scheme with $L = 1$, $L = 10$, and $L = 15$ compared with the conventional DCO-OFDM and COM-based scheme after 20-km SSMF transmission.

Since the permutation matrices used in the encryption were different for different OFDM symbols, this improvement could be attributed to the coding gain from the permutation matrices.

To test the effectiveness of the permutation matrices, we have then investigated the transmission performance of COM- and CNOM-based encryption with and without permutation, as shown in Fig. 7. We can see from Fig. 7(a) that both the COM and CNOM show performance improvement with permutation compared with the cases without permutation, indicating its coding gain. This improvement can be explained by Fig. 7(b). Due to frequency roll-off, which is mainly caused by the joint effect of fiber dispersion and the bandwidth limitation from devices, the signal without a permutation matrix shows a large fluctuation of SNR distribution among subcarriers. Nevertheless, with the help of permutation matrices, a relatively flat SNR distribution can be achieved, leading to a noticeable improvement in transmission performance. Specifically, the CNOM signals without permutation show the worst performance due to additional ICI. However, for

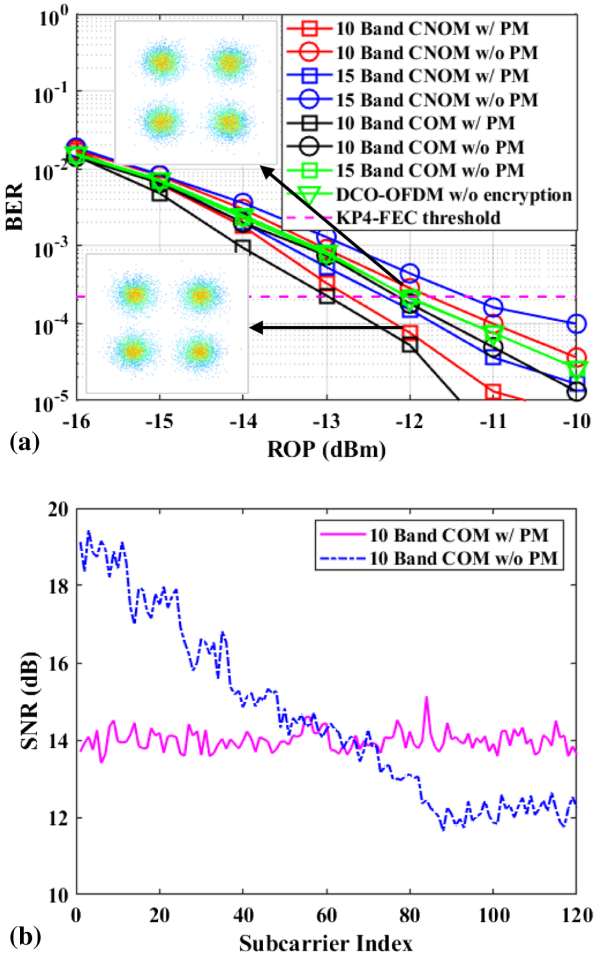

Fig. 7. (a) BER performance of the proposed encryption scheme with and without a permutation matrix (PM). (b) Estimated SNR versus the index of subcarriers for the encrypted signal with and without using a permutation matrix (ROP = −10 dBm).

the same L, the CNOM signal has little performance penalty compared to the COM signal when both employ permutation matrices.

5. SUMMARY

We have experimentally demonstrated a novel multi-band CNOM-based encryption scheme for secure OFDM-PONs. Due to the utilization of non-orthogonality and the multi-band structure, the proposed method can significantly increase the key space and reduce computational complexity compared with the conventional single-band COM/CNOM-based encryption. Moreover, to balance the trade-off among the key space, computational complexity, and transmission performance, we have also investigated the impact of the sub-band number and the corresponding dynamic range on both the transmission and security performance via both simulation and experiment. By employing the proposed multi-band CNOM encryption with the optimal dynamic range, the key space can be increased by 1.4×10^{482} and 1.72×10^{653} times, respectively; the complexity of complex-valued multiplication can be reduced by 90% and 93.33%, respectively; and the complexity of complex-valued addition can be reduced by 90.76% and 94.12%, respectively, in encrypting one OFDM symbol, when the number of sub-bands was increased from 1 (single-band) to 10 and 15, respectively. Moreover, the coding gain from permutation matrices used in the proposed encryption has been validated in a bandwidth-limited channel. All results have indicated the great potential of the proposed multi-band CNOM-based encryption for future high-security and high-speed PONs.

Funding. Research Grants Council, University Grants Committee (GRF 14205820).

Acknowledgment. Portions of this work were presented at the European Conference on Optical Communication (ECOC) in 2022 in paper Tu3B.4.

REFERENCES

1. Y. Shao, R. Deng, J. He, K. Wu, and L. Chen, "Real-time 2.2-Gb/s water-air OFDM-OWC system with low-complexity transmitter-side DSP," J. Lightwave Technol. **38**, 5668–5675 (2020).
2. N. Cvijetic, "OFDM for next-generation optical access networks," J. Lightwave Technol. **30**, 384–398 (2012).
3. J. Wei, C. Sánchez, R. Giddings, E. Hugues-Salas, and J. Tang, "Significant improvements in optical power budgets of real-time optical OFDM PON systems," Opt. Express **18**, 20732–20745 (2010).
4. H. Yang, J. Li, B. Lin, Y. Wan, Y. Guo, L. Zhu, L. Li, Y. He, and Z. Chen, "DSP-based evolution from conventional TDM-PON to TDM-OFDM-PON," J. Lightwave Technol. **31**, 2735–2741 (2013).
5. L. Liu, X. Tang, X. Jiang, Z. Xu, F. Li, Z. Li, H. Huang, P. Ni, L. Chen, L. Xi, and X. Zhang, "Physical layer encryption scheme based on cellular automata and DNA encoding by hyper-chaos in a CO-OFDM system," Opt. Express **29**, 18976–18987 (2021).
6. S. Li, M. Cheng, L. Deng, S. Fu, M. Zhang, M. Tang, P. Shum, and D. Liu, "Secure strategy for OFDM-PON using digital chaos algorithm with fixed-point implementation," J. Lightwave Technol. **36**, 4826–4833 (2018).
7. B. Liu, L. Zhang, X. Xin, and N. Liu, "Piecewise chaotic permutation method for physical layer security in OFDM-PON," IEEE Photon. Technol. Lett. **28**, 2359–2362 (2016).
8. M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Trans. Inf. Forensics Secur. **6**, 725–736 (2011).
9. A. Harris, D. R. Jones, K. H. Horbatuck, and A. Sierra, "A novel wavelength hopping passive optical network (WH-PON) for provision of enhanced physical security," J. Opt. Commun. Netw. **4**, 289–295 (2012).
10. Z. Hu and C. K. Chan, "A real-valued chaotic orthogonal matrix transform-based encryption for OFDM-PON," IEEE Photon. Technol. Lett. **30**, 1455–1458 (2018).
11. Z. Hu and C. K. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON," J. Lightwave Technol **36**, 3373–3381 (2018).
12. Z. Hu, P. Song, and C. K. Chan, "Chaotic non-orthogonal matrix-based encryption for secure OFDM-PONs," IEEE Photon. Technol. Lett. **33**, 1127–1130 (2021).
13. Z. Yang, J. Ke, Q. Zhuge, W. Hu, and L. Yi, "Coherent chaotic optical communication of 30 Gb/s over 340-km fiber transmission via deep learning," Opt. Lett. **47**, 2650–2653 (2022).
14. Z. Yang, L. Yi, J. Ke, Q. Zhuge, Y. Yang, and W. Hu, "Chaotic optical communication over 1000 km transmission by coherent detection," J. Lightwave Technol. **38**, 4648–4655 (2020).
15. M. Cui, Y. Chen, C. Zhang, X. Liang, T. Wu, S. Liu, H. Wen, and K. Qiu, "Chaotic RNA and DNA for security OFDM-WDM-PON and dynamic key agreement," Opt. Express **29**, 25552–25569 (2021).
16. T. Wu, C. Zhang, C. Chen, H. Hou, H. Wei, S. Hu, and K. Qiu, "Security enhancement for OFDM-PON using Brownian motion and chaos in cell," Opt. Express **26**, 22857–22865 (2018).

17. X. Huang, L. Zhang, W. Hu, J. P. Turkiewicz, E. Leitgeb, and X. Yang, "Secure OFDM-PON using chaotic constellation mapping and probabilistic shaping," IEEE Photon. Technol. Lett. **33**, 1139–1142 (2021).
18. 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," Opt. Lett. **45**, 4960–4963 (2020).
19. P. Song, Z. Hu, and C. K. Chan, "An experimental demonstration of secure OFDM-PONs using multi-band chaotic non-orthogonal matrix-based encryption," in *European Conference on Optical Communication*, Basel, Switzerland, 2022, paper Tu3B.4.
20. Z. Hu and C. K. Chan, "Non-orthogonal matrix precoding based faster-than-Nyquist signaling over optical wireless communications," in *Optical Fiber Communication Conference* (Optica Publishing Group, 2020), paper M1J. 5.
21. S. Ohno and G. B. Giannakis, "Optimal training and redundant precoding for block transmissions with application to wireless OFDM," IEEE Trans. Commun. **50**, 2113–2123 (2002).
22. J. Huang, Q. Sui, Z. Li, and F. Ji, "Experimental demonstration of 16-QAM DD-SEFDM with cascaded BPSK iterative detection," IEEE Photon. J. **8**, 7903709 (2016).
23. 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 **61**, 854–864 (2014).
24. F. Uhlig, "Constructive ways for generating (generalized) real orthogonal matrices as products of (generalized) symmetries," Linear Algebra Appl. **332-334**, 459–467 (2001).
25. 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. **12**, 7201215 (2020).
26. L. Zhang, B. Liu, X. Xin, Q. Zhang, J. Yu, and Y. Wang, "Theory and performance analyses in secure CO-OFDM transmission system based on two-dimensional permutation," J. Lightwave Technol. **31**, 74–80 (2013).

Peiji Song received the B.S. degree in optoelectronic information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2019, and he is pursuing his Ph.D. degree in information engineering at The Chinese University of Hong Kong, Hong Kong. His research interests include physical-layer security in PONs, advanced modulation formats, and DSP for optical systems.

Zhouyi Hu received the B.S. degree in optoelectronic information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2016, and the Ph.D. degree in information engineering from The Chinese University of Hong Kong, Hong Kong, in 2020. From 2019 to 2020, he was also with University College London, London, UK, as a Visiting Researcher. From October 2020 to November 2020, he was a Research Associate with The Chinese University of Hong Kong. In December 2020, he joined AiPT, Aston University, Birmingham, UK, as a Research Associate. His research interests include physical-layer security in PONs, optical wireless communications, advanced modulation formats, and DSP for optical systems.

Calvin Chun-Kit Chan received the B.Eng., M.Phil., and Ph.D. degrees in information engineering from The Chinese University of Hong Kong, Hong Kong. Upon graduation, he joined the Department of Electronic Engineering, The City University of Hong Kong, Hong Kong, as a Research Assistant Professor. Later, he joined the Bell Laboratories, Photonic Networks Department, Lucent Technologies, Crawford Hill Holmdel, NJ, USA, as a Member of the Technical Staff. He was a Senior Optical System Engineer with Jedai Broadband Networks, Inc., Red Bank, NJ, USA, before he joined the Department of Information Engineering, The Chinese University of Hong Kong, where he is currently a Professor. He has authored or coauthored more than 320 technical papers in refereed international journals and conferences. He holds two issued US patents, one edited book, and two book chapters. His main research interests include WDM optical metro or access networks, high-speed optical and digital signal processing, optical performance monitoring, and optical network planning and optimization. He was the Co-Chair and a TPC Member for a number of international conferences, including OFC, OECC, CLEO/Pacific Rim, and ACP. He was an Associate Editor for the OSA *Journal of Optical Networking*, IEEE/OSA *Journal of Optical Communications and Networking*, and *Frontiers in Optoelectronics*. He is an Optica Fellow.