Optics Letters

Intrusion detection-embedded chaotic encryption via hybrid modulation for data center interconnects

Wenjun Zeng,[1] Chongfu Zhang,[1,*] Xinshuai Liang,[1] Jiebing Xia,[1] Yue Lin,[1] and Yiting Lin[2]

[1]Key Lab of Optical Fiber Sensing and Communications (MOE), School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]Guangdong Provincial/Zhuhai Key Laboratory of Interdisciplinary Research and Application for Data Science, Beijing Normal-Hong Kong Baptist University, Zhuhai 519087, China
*cfzhang@uestc.edu.cn

Received 29 April 2025; revised 10 June 2025; accepted 10 June 2025; posted 11 June 2025; published 27 June 2025

We propose a chaotic encryption scheme embedded with intrusion detection to safeguard against unauthorized optical access in data center interconnects (DCIs). A hybrid modulation scheme is designed, combining two different modulation methods to achieve dynamic spectral efficiency by adjusting a segmentation parameter. Furthermore, a chaotic hybrid symbol permutation method is introduced to disrupt the distribution characteristics of the constellation sets. An intrusion detection mechanism based on two-stage constellation same-set ratio testing is proposed, using confidence intervals to distinguish between legitimate and unauthorized signals. Finally, the encrypted 56 Gbaud signal is verified over an 80 km link. The results demonstrate that the proposed scheme can effectively detect unauthorized optical access and provide adjustable spectral efficiency, thereby enhancing the resistance of DCIs to optical intrusion.

https://doi.org/10.1364/OL.566608

The rapid advancement of cloud computing has driven the widespread deployment of distributed data centers (DCs). These DCs are interconnected through distributed architectures, forming logically unified resource pools capable of supporting large-scale data processing. Data center interconnects (DCIs) enable data collaboration and high-capacity transmission between DCs by utilizing coherent optical communication systems. However, the dense interconnection of DCs introduces significant security vulnerabilities [1,2]. Attackers can exploit optical eavesdropping techniques and unauthorized access points to intercept and manipulate optical signals, posing substantial risks to DCI transmission security [3].

Currently, physical-layer chaotic encryption techniques are widely employed in optical communication networks [4]. These schemes are integrated with communication technologies, utilizing the high randomness of chaotic maps during digital signal processing (DSP) stages to enhance communication security [5]. For example, Ali *et al.* [6] proposed a chaotic polar coding method to improve both security and transmission performance in cloud-based control systems. In addition, constellation shaping techniques [7,8] and high-dimensional modulation [2] have been incorporated into chaotic encryption schemes to disrupt constellation symbol data. Among these approaches, four-dimensional (4D) modulation [9] offers advantages such as straightforward implementation and strong compatibility, albeit at the expense of reduced spectral efficiency. While constellation probability shaping can mitigate nonlinear effects, it results in a non-uniform distribution of symbol data. Furthermore, multi-level chaotic encryption schemes [10,11] have been proposed to enhance security performance. Collectively, these chaotic encryption approaches provide an effective countermeasure against optical eavesdropping. However, existing schemes lack robustness against active attacks, such as unauthorized optical access. Although chaotic encryption can be combined with conventional intrusion detection methods, current solutions often require additional signal detection hardware [12], thereby increasing deployment costs. Moreover, detection accuracy is susceptible to interference from channel noise. Given that DCs operate under stringent cost constraints, developing a low-cost intrusion detection mechanism integrated with chaotic encryption could provide a cost-effective security enhancement for DCIs.

To address these challenges we propose a chaotic encryption scheme with embedded intrusion detection based on hybrid modulation. The approach enables tunable spectral efficiency by combining two-dimensional (2D) and 4D modulation formats. Subsequently, a chaotic hybrid symbol permutation method is introduced to randomly perturb the distribution of hybrid symbols. Leveraging the unique constellation set properties of 4D modulation, we define an intrusion detection metric termed the constellation same-set ratio (CSSR). An intrusion detection mechanism based on two-stage CSSR testing is designed. Finally, the proposed scheme is validated over an 80 km standard single-mode fiber (SSMF) link.

Figure 1 shows the principle of the proposed chaotic encryption scheme in the DCI. We employ the 2D logistic tent modular map (2D LTMM) [13] to generate chaotic sequences, and its

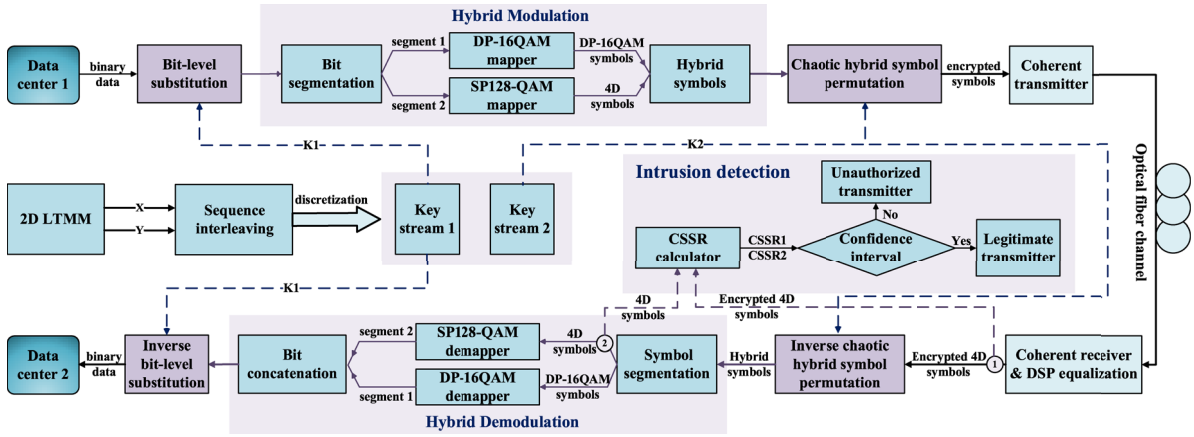

Fig. 1. Implementation principle of the proposed chaotic encryption scheme for DCIs.

model is shown in

$$\begin{cases} x_{i+1} = \begin{cases} \mathrm{mod}(4ax_i(1-x_i)+2by_i,\ 1),\ y_i<0.5 \\ \mathrm{mod}(4ax_i(1-x_i)+2b(1-y_i),\ 1),\ y_i \geq 0.5 \end{cases} \\ y_{i+1} = \begin{cases} \mathrm{mod}(4ay_i(1-y_i)+2bx_i,\ 1),\ x_i<0.5 \\ \mathrm{mod}(4ay_i(1-y_i)+2b(1-x_i),\ 1),\ x_i \geq 0.5 \end{cases} \end{cases}, \tag{1}$$

where a and b are control parameters. When their values lie within the range [1, 100], the system exhibits chaotic behavior. The function $\mathrm{mod}(\cdot,\cdot)$ represents a modulo operation, where the first parameter is the dividend and the second parameter is the divisor. We employ sequence interleaving to connect the x and y sequence outputs to enhance randomness, as shown in

$$Z = [x_1,\ y_1,\ x_2,\ y_2, \ldots,\ x_n,\ y_n]. \tag{2}$$

Based on Eq. (2), two different sets of control parameters and initial values are used to generate the Z_1 and Z_2 sequences. These sequences are then discretized, as shown in

$$K_1 = \mathrm{mod}(\mathrm{floor}(Z_1 \cdot 10^{15}), 2), \tag{3}$$

$$K_2 = \mathrm{sortA}(Z_2), \tag{4}$$

where $\mathrm{floor}(\cdot)$ is a function that rounds a given value down to the largest integer not greater than the value and $\mathrm{sortA}(\cdot)$ returns the index array corresponding to the ascending order of the matrix elements.

The basic encryption model embedded with the intrusion detection mechanism includes bit-level substitution and chaotic hybrid symbol permutation. The implementation method of the bit-level substitution is shown in

$$C_1 = P_1 \oplus K_1, \tag{5}$$

where P_1 represents binary plaintext data and $\oplus$ denotes the exclusive OR (XOR) operation. This process ensures that the data are evenly distributed.

The 128-ary set partitioning 16-quadrature amplitude modulation (SP128-QAM) is a 4D modulation format. While it increases the Euclidean distance between symbols, its spectral efficiency is lower than the 8 bits/symbol of the dual polarization 16-quadrature amplitude modulation (DP-16QAM), which is reduced to 7 bits/symbol. To address this issue, the proposed hybrid modulation divides the bit sequence into two segments, each using a different modulation format, and then concatenates these modulation symbols, as shown in Fig. 2.

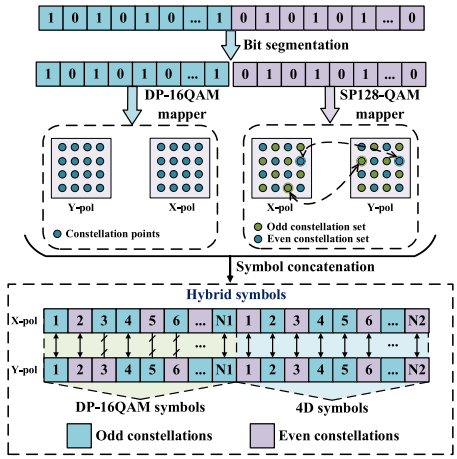

Fig. 2. Schematic diagram of hybrid modulation. Pol: polarization.

A segmented parameter N is introduced to determine the proportion of sequences using 4D modulation, thereby enabling the adjustment of spectral efficiency. The spectral efficiency of the hybrid modulation is calculated as $(1-N)\cdot S_1 + N \cdot S_2$, where S_1 and S_2 represent the spectral efficiencies of 2D and 4D modulation, respectively.

The SP128-QAM divides the 16QAM constellation plane into odd and even constellation sets. Based on this, we introduce a new parameter named CSSR, as shown in

$$\begin{cases} CSSR = \frac{1}{M}\sum_{i=1}^{M} Q(i) \\ Q(i) = \begin{cases} 0, if\ C_X(i) \neq C_Y(i) \\ 1, if\ C_X(i) = C_Y(i) \end{cases} \end{cases}, \tag{6}$$

where M is the length of the 4D symbols. $Q(i)$ is an identifier, where $Q(i) = 1$ if the ith constellation symbols $C_X(i)$ and $C_Y(i)$ of the X- and Y-polarization branches belong to the same constellation set and $Q(i) = 0$ otherwise. The SP128-QAM symbols all belong to the same constellation set, while the constellation set distribution of DP-16QAM symbols is random. We design a chaotic hybrid symbol permutation method to disrupt the distribution of this constellation set, as shown in

$$C_2 = \mathrm{sort}(H, K_2), \tag{7}$$

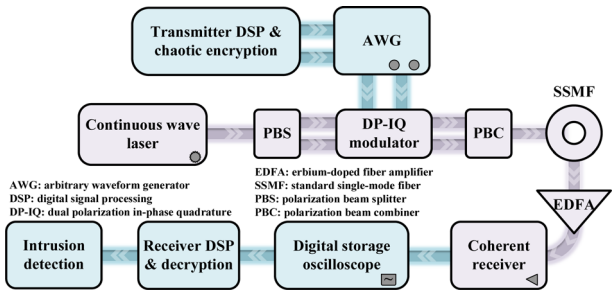

Fig. 3. Communication setup of the proposed scheme.

where H is the hybrid symbol sequence. sort$(\cdot,\cdot)$ denotes a sorting function, where the first parameter is the sequence to be sorted, and the second parameter specifies the sorting indices. Due to the randomness of the chaotic key, the constellation set distribution of the hybrid symbol sequence after permutation also becomes random. At the receiver, the original constellation distribution can be restored by inverse chaotic hybrid symbol permutation.

The intrusion detection mechanism is based on a two-stage CSSR test, which evaluates the CSSR values before and after the inverse chaotic hybrid symbol permutation, denoted as CSSR1 and CSSR2, respectively. We then establish corresponding confidence intervals for CSSR1 and CSSR2 to mitigate the impact of channel noise. The calculation method for the confidence interval of CSSR1 is shown in

$$\begin{cases} C_1^- = \mu_1 - |\phi^{-1}(\alpha/2)| \cdot \sigma_1 \\ C_1^+ = \mu_1 + |\phi^{-1}(\alpha/2)| \cdot \sigma_1 \end{cases}, \tag{8}$$

where $\mu_1 = p_1$ and $\sigma_1 = \sqrt{p_1(1-p_1)/M}$ are the expectation and standard deviation of CSSR1, respectively. p_1 represents the probability of $Q = 1$, with a value of 0.5 for a random constellation set. $\phi^{-1}(\cdot)$ is the inverse cumulative distribution function of the normal distribution, and α is the significance level. The confidence interval calculation method for CSSR2 is shown in

$$C_2 = \mu_2 - |\phi^{-1}(\alpha)| \cdot \sigma_2, \tag{9}$$

where μ_2 and σ_2 are the expectation and standard deviation of CSSR2, respectively. CSSR2 requires testing the symbol error rate (SER) performance of the actual channel. We use the upper bound φ of the SER confidence interval to derive the confidence interval of CSSR2, thereby improving noise tolerance. The probability of $Q = 1$ can be defined as $p_2 = (1-\varphi)^2$ in CSSR2 testing. Then, the expectation and standard deviation of CSSR2 can be calculated by $\mu_2 = p_2$ and $\sigma_2 = \sqrt{p_2(1-p_2)/M}$. The discrimination criteria for legitimate signals are that both CSSR1 and CSSR2 fall within their respective confidence intervals.

Figure 3 illustrates the setup of the proposed scheme. The baud rate of the proposed scheme is 56 Gbaud, and the length of the SSMF is 80 km. We employ 10 sets of pseudo-random bit sequences (PRBS) to test the channel SER performance to determine φ. The segmented parameter N can be set to 0.75, 0.5, 0.25, and 0.125. The symbol length of a single polarization channel is fixed at 65536, and PRBS data is used as the transmitted data.

Figures 4(a) and 4(b) illustrate the CSSR1 and CSSR2 characteristics under different segmentation parameters N. Due to the variations in N, the length of the 4D symbols changes, resulting in different confidence intervals. Specifically, a decrease in N expands the confidence interval of CSSR1 and lowers the lower bound of the confidence interval for CSSR2. This is because reducing N shortens the length M of the 4D symbol, which increases the standard deviation of both CSSR1 and CSSR2. Consequently, decreasing N enhances the tolerance of the intrusion detection mechanism to noise. The CSSR1 and CSSR2 of signals with different segmentation parameters remain within their respective confidence intervals. CSSR1 is unaffected by the optical signal-to-noise ratio (OSNR), and the randomness of noise causes the distribution of constellation sets to approach randomness. In contrast, CSSR2 is primarily influenced by the SER, and a decrease in OSNR exacerbates the degradation of SER. Therefore, CSSR2 is a noise-sensitive parameter.

Figures 4(c) and 4(d) present the intrusion detection results for legitimate and unauthorized transmitters. The legitimate transmitter adopts the proposed scheme with $N = 0.5$. Unauthorized transmitters include attackers using three modulation scenarios: DP-16QAM modulation, SP128-QAM modulation, and the proposed scheme without the correct encryption key. Except for the CSSR1 of unauthorized transmitters modulated with SP128-QAM, which does not fall within the confidence interval, the CSSR1 of all other signals falls within the confidence range. However, this does not imply that they can be recognized as legitimate signals, as the decision criteria also depend on CSSR2. Only the CSSR2 of the legitimate transmitter falls within the confidence interval. Since unauthorized signals are not encrypted by legitimate encryption devices, the distribution of constellation sets tends to be random after inverse chaotic hybrid symbol permutation at the receiver, resulting in CSSR2 approaching 0.5. Therefore, the two-stage CSSR intrusion detection mechanism can effectively identify unauthorized optical access signals. Moreover, the proposed scheme demonstrates effective intrusion detection capabilities under various OSNR conditions, indicating that the intrusion detection mechanism is less susceptible to channel noise.

Figure 4(e) shows the bit error rate (BER) performance comparison results. The spectral efficiency is 7.875 bits/symbol when $N = 0.125$, corresponding to a bit rate of 441 Gbit/s (56 Gbaud × 7.875 bits/symbol). The traditional DP-16QAM scheme is compared with the proposed scheme at $N = 0.125$, operating at the same baud rate and bit rate. The results indicate that increasing the N value improves the BER performance of the system. This is because a higher N value increases the proportion of 4D modulation symbols in the hybrid modulation, benefiting from the enhanced performance of 4D modulation. However, increasing N reduces the spectral efficiency. For example, when $N = 0.75$, the spectral efficiency is 7.25 bits/symbol, which is 0.625 bits/symbol lower than that at $N = 0.125$. Compared to the traditional DP-16QAM scheme, the proposed hybrid modulation scheme demonstrates superior BER performance at both the same baud rate and bit rate. Additionally, attackers are unable to decrypt the information correctly due to the absence of the key, resulting in a BER approaching 0.5.

The proposed scheme utilizes two encryption key sequences, K_1 and K_2. These key parameters are perturbed with a perturbation amplitude of 10^{-14}, and the changes in CSSR2 and BER following the perturbation are then evaluated. Figure 4(f) shows the sensitivity test results for the key parameters. CSSR2 is only influenced by K_2, as only the chaotic hybrid modulation permutation alters the distribution of constellation sets. Any disturbance in the key parameters of either K_1 or K_2 causes the BER to approach 0.5. This demonstrates that the key parameters of

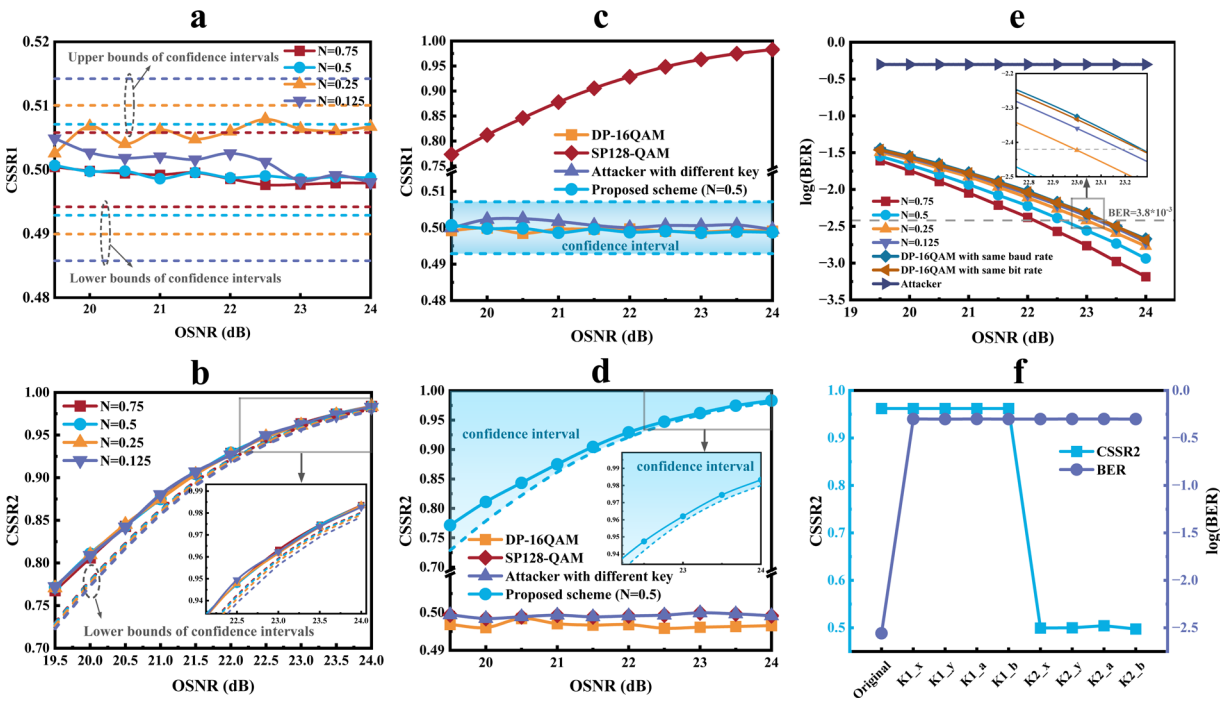

Fig. 4. Intrusion detection and security test results of the proposed scheme. (a) and (b) show the CSSR1 and CSSR2 characteristics under different segmentation parameters, respectively. (c) and (d) present the intrusion detection results for legitimate and unauthorized transmitters. (e) illustrates the BER results. (f) displays the sensitivity test results of chaotic key parameters, and K1_x represents the K_1 generated by changing only the parameter x.

Table 1. Comparisons with Existing Chaotic Encryption Schemes

Scheme	Key Space	Anti-Unauthorized Access	Complexity
[6]	2.245×10^{75}	×	$O(N^2)$
[14]	10^{45}	×	O(N)
[15]	10^{127}	×	O(N)
Proposed	10^{120}	√	O(N)

the proposed scheme are highly sensitive, ensuring robust protection for both the confidentiality of DCI data transmission and the effectiveness of intrusion detection.

Table 1 provides a comparative analysis of the proposed scheme with existing schemes [6,14,15]. The key space (four initial parameters and four control parameters, $10^{14\times4+16\times4} = 10^{120}$) of the proposed scheme is sufficiently large to withstand brute-force attacks, while its computational complexity remains low. A notable advantage of the proposed scheme is its embedded intrusion detection mechanism, which enables the detection of unauthorized access attacks—an ability not provided by existing schemes. Furthermore, the intrusion detection method does not impact decryption efficiency and can be selectively activated.

In summary, we proposed and validated an intrusion detection-embedded chaotic encryption scheme based on hybrid modulation for DCIs. Transmitted data can be uniformly and randomly perturbed. The hybrid modulation can provide adjustable spectral efficiency, mitigating the spectral efficiency reduction issue associated with 4D modulation. The intrusion detection mechanism can accurately identify unauthorized optical access. The proposed scheme provides a secure solution for DCIs, enhancing resistance to both optical eavesdropping and unauthorized access.

Funding. Natural Science Foundation of Sichuan Province (2025ZNSFSC0491).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. B. Zhu, F. Wang, and J. Yu, IEEE Photonics Technol. Lett. **33**, 383 (2021).
2. W. Zeng, C. Zhang, X. Liang, *et al.*, IEEE Trans. Ind. Inform. **21**, 1259 (2025).
3. N. Skorin-Kapov, M. Furdek, S. Zsigmond, *et al.*, IEEE Commun. Mag. **54**, 110 (2016).
4. L. Liu, X. Tang, F. Li, *et al.*, J. Lightwave Technol. **41**, 6507 (2023).
5. Y. Wang, Q. Zhang, X. Xin, *et al.*, J. Opt. Commun. Netw. **16**, 1204 (2024).
6. Y. Ali, Y. Xia, W. Sułek, *et al.*, IEEE Trans. Ind. Inform. **20**, 3935 (2024).
7. Z. Wang, Y. Xiao, S. Wang, *et al.*, Opt. Express **29**, 17890 (2021).
8. W. Zeng, C. Zhang, X. Liang, *et al.*, Opt. Express **32**, 1595 (2024).
9. K. Wang, J. Yu, P. Gou, *et al.*, Opt. Fiber Technol. **43**, 158 (2018).
10. M. Li, B. Liu, R. Ullah, *et al.*, Opt. Lett. **45**, 4960 (2020).
11. J. Wang, B. Liu, J. Ren, *et al.*, Opt. Lett. **50**, 285 (2025).
12. K. Abdelli, H. Grießer, and C. Tropschug, J. Lightwave Technol. **40**, 2254 (2022).
13. Z. Hua, Z. Zhu, S. Yi, *et al.*, Inf. Sci. **546**, 1063 (2021).
14. T. Wu, W. Zhu, Y. Liu, *et al.*, J. Lightwave Technol. **42**, 8152 (2024).
15. Y. Chen, J. Chen, M. Zhang, *et al.*, Opt. Express **31**, 3153 (2023).