Optics EXPRESS

Convex optimization-based high-speed and security joint optimization scheme in optical access networks

ANQI HU,[1] LU GAN,[2] LEI GUO,[1] HAO YAN,[3] AND JUNFAN HU[4]

[1] *School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[2] *Department of Electronic and Electrical Engineering College of Engineering, Design and Physical Science, Brunel University London, London UB8 3PH, UK*
[3] *Department of Electrical and Electronic Engineering, Imperial College London, London, SW7 2AZ, UK*
[4] *State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*

Abstract: Data rate and security are essential performance metrics for passive optical networks (PON). However, existing optical access networks lack standardized metrics to evaluate rate and security performance uniformly. This paper introduces a high-speed and security joint optimization scheme for optical access networks using convex optimization. Evaluation metrics for data rate and security performance in PON are established. According to the evaluation metrics, the security optimization objective function U_s, high-speed optimization objective function *GMI*, and high-speed security joint-optimization objective function H_s are established. An optimization problem is formulated to maximize weighted rate and security indicators, factoring in constraints such as maximum power, probability, amplifier capacity, normalized mutual information, and key and frame lengths. An alternating optimization method is applied to iteratively address sub-problems by exploiting successive convex approximations and differences of convex functions. This transforms non-convex sub-problems into convex optimizations. Experimental results highlight notable improvements in objective function values, confirming the effectiveness of the proposed high-speed security optimization algorithm for optical access networks.

1. Introduction

The surge in Internet of Things, cloud computing, and 4K/8K video services has heightened bandwidth demands for optical access networks. Passive optical networks (PON) utilize a point-to-multipoint tree topology, offering a high-bandwidth, cost-efficient network solution [1,2]. While strategies like coherent detection [3,4], wavelength division multiplexing [5,6], and high-order modulation [7,8] have been employed to enhance PON capacity, they necessitate hardware upgrades, escalating costs and complexity. Optimizing system capacity without incurring added costs or compromising compatibility with current optical communication systems is more pragmatic. Most commercial PON systems deploy fixed data rates, resulting in suboptimal resource use. Moreover, the PON's point-to-multipoint structure means that optical line terminal (OLT) signals broadcast to all optical network units (ONU), posing a potential risk of information leaks. Consequently, tailoring data rates based on channel conditions for capacity augmentation and secure transmission is a focal research area.

Rate adaptation is often achieved through coding modulation. One straightforward method is employing varying modulation orders, essentially altering the rate by modifying the symbols' information entropy. Due to the discontinuous nature of entropy-based rate changes and sensitivity variances between modulation formats, this hasn't gained broad adoption [9]. Another popular rate adaptation technique involves forward error correction (FEC) [10–13]. Designing FECs for

#512191 https://doi.org/10.1364/OE.512191
Journal © 2024 Received 13 Nov 2023; revised 13 Jan 2024; accepted 30 Jan 2024; published 9 Feb 2024

diverse bit rates to suit varying channel conditions offers finer rate adjustment than entropy tuning. Nonetheless, a consistent 1.53 dB gap exists between the uniform signal scheme using FEC and theoretical capacity [14], constraining capacity enhancements. Reference [14] demonstrates this gap can be reduced with the Maxwell-Boltzmann distribution. Subsequent research proposed multiple constellation shaping strategies aiming to achieve Shannon's limit capacity [15–18]. Georg Böcherer introduced the probabilistic amplitude shaping (PAS) architecture in 2015 [19], seamlessly integrating shaping outer code and FEC inner code of distribution matchers. This enhancement boosted probability shaping's system adaptability and facilitated more precise transmission rate adjustments than with FEC alone. The PAS-based rate-adaptive scheme garnered significant attention, with works such as [20] and [21] deriving optimal parameters for probabilistic shaping (PS) and FEC from an informational theory perspective. Further, [22] provides a clearer display of the PS and FEC integration, analyzing their optimal combination. On the other hand, [23] highlights the performance degradation introduced by PAS's pairing constraint and suggests geometric shaping (GS) to mitigate such losses. Notably, while these strategies excel in optimizing PS and FEC, they often overlook security considerations specific to PON networks.

For security, electric domain-based physical layer encryption aligns well with the high-speed, cost-efficient, and secure demands of PON networks for data protection, making it a popular choice for PON security schemes. Chaotic encryption, a subset of these encryption strategies, is favored due to its acute sensitivity to initial values and control parameters, satisfying cryptographic needs for confusion and diffusion [24]. Multiple physical layer chaotic encryption methods have been introduced recently, showcasing their distinct data protection merits [25–30]. However, many primarily emphasize security, neglecting holistic system performance. Several strategies [25,31,32] addressed the security and rate optimization of PONs independently. However, there is a deficiency in achieving a unified evaluation and balance in coordinating and optimizing the overall performance. To achieve a balanced system prioritizing effectiveness, reliability, and security, it's imperative to evaluate and harmonize encryption techniques with communication coding and modulation strategies.

This paper addresses the above-mentioned challenges in PON, by introducing a novel high-speed and security joint optimization approach. The primary contributions include:

- **Novel Joint Optimization Scheme**: Introducing a convex optimization-based high-speed and security scheme for PON that takes into account both rate and security.
- **Metric Quantification**: Quantifying PON rate using generalized mutual information (GMI), and establishing new security metrics.
- **Objective Function Construction**: Establishment of a security objective function U_s, the high-speed optimization objective function GMI and a high-speed security objective function H_s that weigh security and communication quality.
- **Complex Problem Decomposition**: The formulation of a comprehensive optimization problem with real-world constraints is divided into manageable sub-problems using alternating optimization.
- **Practical Solution**: Leveraging techniques like successive convex approximation (SCA) and the difference of convex functions (DC) to transform these sub-problems, leading to practical solutions backed by extensive simulations that validate the effectiveness of the proposed approach.

The remaining part of this paper is organized as follows. In Section 2, the principle of optimizing PON system, the metrics of rate and security are introduced. According to the metrics of rate and security, the safety optimization objective function U_s, the high-speed optimization objective function *GMI* and a high-speed security optimization objective function H_s is constructed to weigh the security and quality of communication, and the optimization problem is solved by alternating optimization method. In Section 3, the optimized chaotic encryption and hybrid probability geometric shaping of 16QAM (HPGS-16QAM) signal transmission are simulated in the PON simulation system. Through the simulation comparison of controlling the number of optimization variables, the effectiveness of the joint high-speed and security optimization algorithm of optical access network based on convex optimization is confirmed.Finally, the joint optimization scheme proposed in the paper is summarized and prospected in the Conclusion (Section 4).

2. Optimization scheme for high-speed and security in optical access network

This section introduces the principle of optimization system, the metrics of rate and security, the mathematical modeling of high-speed security optimization problem, the method of decomposing complex optimization problem into several sub-problems by alternating optimization, and transforming each sub-problem into a solvable convex optimization problem to solve.

2.1. Principle of system

Figure 1 shows the diagram of the proposed PON system. Given the uniform distribution of encrypted data and the specific distribution requirement for coded data, this study employs a sequential approach: first encrypting data, followed by coding modulation, with both processes being independent. Within the OLT, input bit data undergoes encryption using a mask, generated via chaotic mapping based on a shared key between OLT and ONU and optimized algorithm parameters. These parameters, stored in the DSP processor, ensure encryption's security and efficacy. Subsequently, the encrypted bit sequence undergoes channel coding, which encompasses an offline optimization phase. Parameters derived from this are applied for constellation shaping and FEC, yielding an optimized M-QAM signal. This signal is then transformed into an optical signal via a photoelectric converter and transmitted through optical fiber. After attenuation by the semiconductor optical amplifier (SOA) and variable optical attenuator (VOA), it reaches the receiver, where the original data is retrieved through a coherent receiver's demodulation.

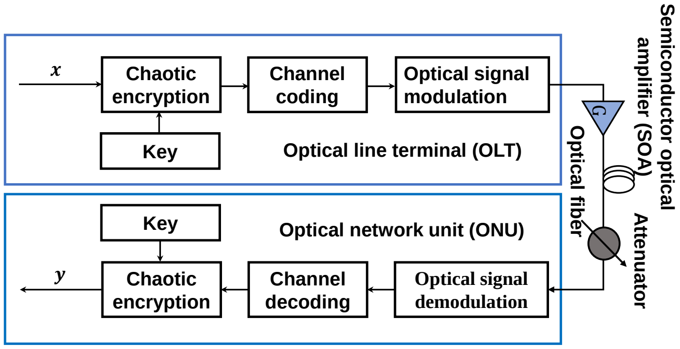
x
Chaotic encryption
Channel coding
Optical signal modulation
Key
Optical line terminal (OLT)
G
Semiconductor optical amplifier (SOA)
Optical fiber
Attenuator
Key
Optical network unit (ONU)
y
Chaotic encryption
Channel decoding
Optical signal demodulation

Fig. 1. The diagram of the proposed high-speed and security PON optimization system.

2.2. Metrics of rate

As illustrated in Fig. 1, assumed that the data x is transmitted at the OLT and after passing through the additive white Gaussian noise (AWGN) channel, the data y is received at the ONU.

The achievable rate can be characterized by GMI [33]:

$$\mathrm{GMI}\left(X;Y\right)=\max\left(H\left(X\right)-\sum_{j=1}^{m}H\left(B_j|Y\right),0\right),\tag{1}$$

where B_j denotes the j-th bit of the symbol. Here, GMI is calculated according to the Gray mapping. Based on the probability theory, in the memoryless AWGN auxiliary channel with noise power σ^2, the probability distribution of a received data y given the transmitted data x is defined by

$$q_{Y|X}\left(y|x\right)=\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{|y-x|^2}{2\sigma^2}}.\tag{2}$$

In the setting of a square M-QAM constellation that can carry at most $m=\log_2 M$ bits/symbol, the GMI under bit-metric decoding (BMD) can be estimated as [34]

$$\mathrm{GMI}\approx-\sum_{x\in X}P_X\left(x\right)\log_2 P_X\left(x\right)+\frac{1}{N}\sum_{k=1}^{N}\sum_{i=1}^{m}\log_2\frac{\sum_{x\in\mathcal{X}_{b_{k,i}}}q_{Y|X}\left(y_k|x\right)P_X\left(x\right)}{\sum_{x\in\mathcal{X}}q_{Y|X}\left(y_k|x\right)P_X\left(x\right)},\tag{3}$$

where $\mathcal{X}$ represents the set of M-QAM symbols, $b_{k,i}\in\{0,1\}$ denotes the i-th bit of the k-th transmit symbol, and $\mathcal{X}_{b_{k,i}}$ is the set of the M-QAM symbols whose i-th bit value is $b_{k,i}$. It worth noting that the GMI quantifies the maximum number of information bits per transmit symbol in the bit-interleaved coded modulation AWGN auxiliary channel, with ideal binary forward error correction decoding. Once the GMI is estimated, the maximum number of information bits per transmit bit is obtained for uniform M-QAM by a simple normalization [34]

$$\mathrm{NGMI}=1-(H(X)-\mathrm{GMI})/m,\tag{4}$$

where $0\leq\mathrm{NGMI}\leq1$.

2.3. Metrics of security

In this paper, we focus not only on the rate improvement in the PON, but also its security. We use two one-dimensional modified chaotic maps to encrypt the transmitted data [35]. The method of generating mask sequence by cross-mapping is shown in Fig. 2, where c represents the number of cross-mappings and n represents the number of chaotic pre-iterations. X_1 represents the initial value of the modified Logistic map, while U_1 denotes the initial value of the modified Chebyshev map. The Y map corresponds to the left branch of the cross-mapping, and the Z map corresponds to the right branch. Within the left branch, the control parameter μ_1 and the initial value U_1 undergo computations through the modified Chebyshev map, resulting in the real number y_1. This value is then input into the modified Logistic map with a parameter value of $a=1$, yielding the real number y_2, thereby completing one iteration of cross-mapping in the left branch. A similar sequence of steps is conducted in the right branch, and both branches engage in simultaneous cross-mapping processes. Each chaotic iteration will produce a floating-point number, and different quantization methods can be used to get different bit numbers d. c, n and d are parameters that can be flexibly adjusted in encryption algorithm.

As far as encryption is concerned, security and efficiency are two very important indicators. Security can be quantified by the workload required for cryptanalysis, which is defined as encryption security level by [36]. Encryption efficiency mainly considers the complexity of encryption algorithm and the effectiveness of encryption. In addition, due to the requirement of high-speed PON for real-time communication, we increase the time sensitivity to measure the impact of encryption time on the real-time system.

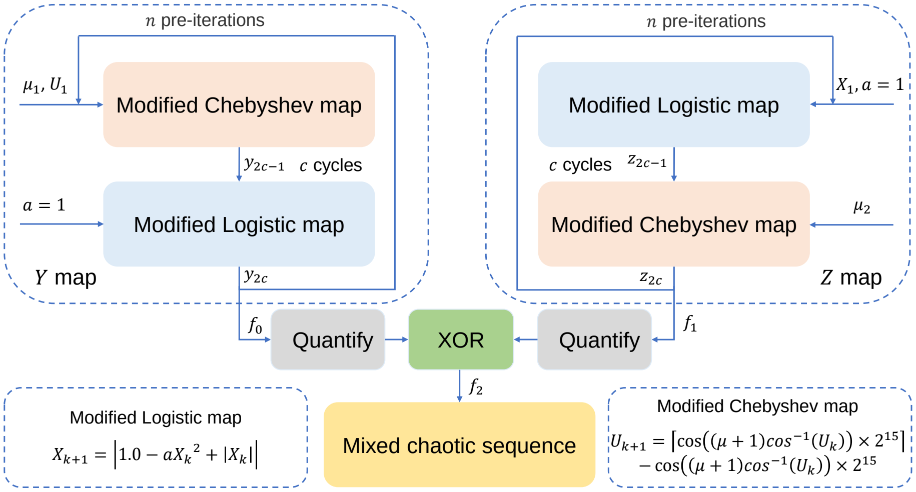

Fig. 2. The diagram of chaotic cross-mapping in chaotic encryption.

Here, we consider using different encryption key lengths K for each possible frame length L in packet encryption. If the same key length is used for all frame lengths, attacks on smaller frame lengths can lead to key leakage. Increasing the frame length does not exponentially enhance the security of the cipher if a portion of the key is compromised. Since the key is changed only once per session and requires thousands of encryption operations before each key change, we aim to minimize the impact on key management complexity as we need to ensure that each frame has a unique encryption key. As shown in Fig. 3, we incorporate a cryptographic key in each frame, serving as the generative factor for the initial conditions of a chaotic mapping. Consequently, the length K of the key introduces redundancy to the transmitted data. In light of ensuring system security and facilitating an efficient data transmission rate, it becomes imperative to establish rational security assessment metrics, thus achieving a balance between security and transmission performance.

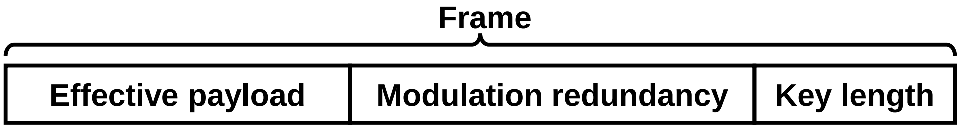

Fig. 3. The structure of the data frame.

To quantify the metrics of security, we establish a security metrics objective function as

$$U_s = s_t \cdot s_u \cdot s_r \cdot s_o, \tag{5}$$

where s_t, s_u, s_r and s_o denote the encryption time sensitivity, encryption effectiveness, encryption security level and encryption complexity, respectively. The encryption time sensitivity can be quantified by

$$s_t = \frac{1}{\log(\rho + 1)}, \tag{6}$$

where ρ is the parameter of encryption complexity, which is related to the numbers of cross mapping c, iterations n and bits of quantization, and is given as

$$\rho = \frac{(2c + n)\alpha L}{2^d}, \tag{7}$$

where α is the running time of chaotic function, L is the length of one frame. The encryption overhead can be measured by the following

$$s_l = \frac{K}{L}, \tag{8}$$

where K is the length of key. Then, the encryption effectiveness can be measured by

$$s_u = 1 - \frac{K}{L}. \tag{9}$$

Obviously, The security level of encryption [36] can be defined as

$$s_r = \log_2 K. \tag{10}$$

Finally, the encryption complexity is determined by the numbers of cross mapping c and iterations n, which is given as

$$s_o = \ln\left(1 + \frac{(2c+n)}{d}\right). \tag{11}$$

In all, the encryption objective function U_s can be represent as

$$U_s = \frac{1}{\log\left(\frac{(2c+n)\alpha L}{2^d} + 1\right)} \cdot \left(1 - \frac{K}{L}\right) \cdot \log_2 K \cdot \ln\left(1 + \frac{(2c+n)}{d}\right). \tag{12}$$

2.4. Objective function

In this study, we aim to construct a high-speed and security PON by optimizing the PS, GS, the length of the frame, and the length of the key. We propose a high-speed security optimization problem, and express the high-speed security objective function H_s by the weighted sum of the maximization rate and the security metrics, and its mathematical formula is as follows

$$\max_{K,L,P_X,S_X} \quad \beta_s U_s + \beta_r \mathrm{GMI}\,(X;Y) \tag{13a}$$

$$\text{s.t.} \quad \psi \cdot G \cdot L \cdot \sum_{i=1}^{m} P_X\,(x_m) \cdot S_X\,(x_m) \leqslant P_{\max} \tag{13b}$$

$$\sum_{i=1}^{m} P_X\,(x_m) = 1 \tag{13c}$$

$$\max\,(\psi \cdot G \cdot X) \leqslant X_{\mathrm{th}} \tag{13d}$$

$$\mathrm{NGMI} \geqslant R_{th} \tag{13e}$$

$$K_{\min} \leqslant K \leqslant K_{\max} \tag{13f}$$

$$L_{\min} \leqslant L \leqslant L_{\max}, \tag{13g}$$

where ψ and G are the amplifier parameters. In the optimization problem (13), (13b)–(13g) are the maximum transmit power, sum of the probability, maximum peak power, minimum NGMI, key and frame length constraints, respectively. The problem is a non-convex optimization problem, and the optimization variables are coupled together, which is difficult to solve directly.

2.5. Alternating optimization algorithm

Alternating optimization method is utilized to solve the optimization problem (13). The Alternating optimization method is to optimize one of the optimization variables while fixing the others, and then iterate among them. Firstly, we optimize the length of the key K.

2.5.1. Optimize key length K

The optimization variable K only appears in the security metrics U_s and the constraint (13f). The sub-problem can be given as

$$\max_{\boldsymbol{K}} \quad \beta_s U_s \tag{14a}$$

$$\text{s.t} \quad (13\text{f}) \tag{14b}$$

Obviously, the constraint (13f) is a linear constraint, which is both convex and concave.

Lemma 2.1 *The security objective function U_s is a concave function with respective to K.*

Proof 2.1 *Define $\chi = \frac{1}{\log\left(\frac{(2c+n)\alpha L}{2^d}+1\right)} \cdot \ln\left(1 + \frac{(2c+n)}{d}\right) > 0$, which is independent of K. Then, $U_s = \chi\left(\log_2 K - \frac{K}{L}\log_2 K\right)$. The second partial derivative of U_s with respect to K is given by*

$$\frac{\partial^{(2)} U_s}{\partial^{(2)} K} = -\frac{\chi}{\ln(2^{K^2})} - \frac{\chi}{\ln(2^{LK})} < 0. \tag{15}$$

Thus, the security metrics U_s is a concave function with respective to K.

The optimization problem (14) is a convex problem, which can be solved directly.

2.5.2. Optimize frame length L

The frame length L is only appears in the security metrics U_s and the constraints (13b) and (13g). The sub-problem can be given as

$$\max_{L} \quad \beta_s U_s \tag{16a}$$

$$\text{s.t.} \quad (13\text{b}), (13\text{g}) \tag{16b}$$

Obviously, the constraints (13b) and (13g) are linear function with respective to L. We mainly focus on the relationship between the objective function and the parameter L. Let $\eta = \log_2 K \cdot \ln\left(1 + \frac{(2c+n)}{d}\right)$, the objective function can be simplified as

$$U_s = \eta\left(\frac{1}{\log\left(\frac{(2c+n)\alpha L}{2^d} + 1\right)} - \frac{K}{L\log\left(\frac{(2c+n)\alpha L}{2^d} + 1\right)}\right), \tag{17}$$

Based on the second order condition, it is easy to find that $\frac{1}{\log\left(\frac{(2c+n)\alpha L}{2^d}+1\right)}$ is a convex function and $\frac{K}{L\log\left(\frac{(2c+n)\alpha L}{2^d}+1\right)}$ is a concave functions. SCA is utilized to solve the problem [37]. To simplify the expression, let $\delta \triangleq \frac{(2c+n)\alpha}{2^d}$, then the first order Taylor expansion of the objective function with respective to L is given as

$$\begin{aligned} U_s\left(\bar{L}, L\right) \approx \eta\Bigg(&\frac{1}{\log(\delta\bar{L}+1)} - \frac{x}{\left(\log\left(\bar{L}x+1\right)\right)^2\left(\bar{L}x+1\right)}\left(L-\bar{L}\right) - \frac{K}{L\log(\delta\bar{L}+1)} \\ &+ \left(\frac{K}{\bar{L}^2\log(\delta\bar{L}+1)} + \frac{K\delta}{\bar{L}\left(\log\left(\delta\bar{L}+1\right)\right)^2\left(\chi\bar{L}+1\right)}\right)\left(L-\bar{L}\right)\Bigg), \end{aligned} \tag{18}$$

where $\bar{L}$ is the value in the last iteration. Here, $U_s\left(\bar{L}, L\right)$ is a linear function of L, which can be solved directly.

2.5.3. Probabilistic shaping

The PS vector P_X is appears in the rate metrics, probability constraint, and NGMI constraint. The sub-problem is give as

$$\max_{P_X} \quad \beta_r \mathrm{GMI}\left(X;Y\right) \tag{19a}$$

$$\text{s.t.} \quad (13\text{b}),\ (13\text{c}), (13\text{e}) \tag{19b}$$

Similarly, the constraints (13b) and (13c) are linearly with respect to P_X. Equation (3) is an estimate of GMI. Obviously, it can be proved that the entropy function $-\sum_{x\in\mathcal{X}} P_X\left(x\right)\log_2 P_X\left(x\right)$ is a concave function. Also, $\log_2\left(\sum_{x\in\mathcal{X}_{b_{k,i}}} q_{Y|X}\left(y_k|x\right)P_X\left(x\right)\right)$ and $\log_2\left(\sum_{x\in\mathcal{X}} q_{Y|X}\left(y_k|x\right)P_X\left(x\right)\right)$ are concave functions. Thus the second part of the GMI is a structure of DC. We can linearize the $\log_2\left(\sum_{x\in\mathcal{X}} q_{Y|X}\left(y_k|x\right)P_X\left(x\right)\right)$ by the first order Taylor expansion as

$$\begin{aligned} &\log_2\left(\sum\nolimits_{x\in\mathcal{X}} q_{Y|X}\left(y_k|x\right)P_X\left(x\right)\right) \\ &\approx \log_2\left(\sum\nolimits_{x\in\mathcal{X}} q_{Y|X}\left(y_k|x\right)\bar{P}_X\left(x\right)\right) + \frac{\sum_{x\in\mathcal{X}} q_{Y|X}\left(y_k|x\right)\left(P_X\left(x\right)-\bar{P}_X\left(x\right)\right)}{\ln 2\sum_{x\in\mathcal{X}} q_{Y|X}\left(y_k|x\right)\bar{P}_X\left(x\right)}. \end{aligned} \tag{20}$$

where $\bar{P}_X$ is the probability vector in the last iteration. NGMI can be dealt with similar method, we omit the procedure here. Then, the sub-problem is a convex problem, which can be solved by the existent convex optimization toolbox, such as CVX.

2.5.4. Geometric shaping

The constraints (13b), (13d) and (13e) have the optimization variable vector S_X, and (13b) is a linear function with respect to S_X, and (13d) is a convex constraint. Then, the sub-problem is rewritten as

$$\max_{S_X} \quad \beta_r \mathrm{GMI}\left(X;Y\right) \tag{21a}$$

$$\text{s.t.} \quad (13\text{b}),\ (13\text{d}),\ (13\text{e}) \tag{21b}$$

Certainly, (13b) is a linear constraint, (13d) is a convex constraint with respect to S_X. As for the objective function and constraint (13e), S_X appears in the Gaussian distribution function (2), similarly, SCA is adopted to linearize the Eq. (2) as follows

$$q_{Y|X} = \frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{|y-x|^2}{2\sigma^2}} \approx \frac{1}{\sqrt{2\pi\sigma^2}}\left(e^{-\frac{|y-\bar{x}|^2}{2\sigma^2}} + \Re\left\{\left(e^{-\frac{|y-\bar{x}|^2}{2\sigma^2}}\cdot\frac{2y-2\bar{x}}{2\sigma^2}\right)^*\left(x-\bar{x}\right)\right\}\right) \tag{22}$$

where $(\cdot)^*$ denotes the conjugate operation. In this way, sub-problem (21) is a convex optimization problem, which can be solved directly.

The overall optimization pseudo-code is summarized in the Algorithm 1.

Algorithm 1. Optimization algorithm for the high-speed and security PON.

```
Input: Initialize: $P_X$ , $S_X$, $L_0$, $c$, $n$, $\alpha$, $d$
Output: optimal $P_X^*$, $S_X^*$, $L^*$, $K^*$
repeat
    Solve the sub-problem (14), and update $K$;
    Solve the sub-problem (16), and update $L$;
    Solve the sub-problem (19), and update $P_X$;
    Solve the sub-problem (21), and update $S_X$;
until $\left\|P_X - \bar{P}_X\right\| \leqslant 1\times 10^{-4}$
```

3. Simulation setup and results

This section introduces the PON simulation system based on chaotic encryption and HPGS-16QAM signal (taking $M = 16$ as an example), and describes the system setup accordingly, and then the simulation results are analyzed and illustrated in detail.

3.1. Simulation setup

As illustrated in Fig. 4, the system simulates the PON based on chaotic encryption and HPGS-16QAM signal, the baud rate is 39 Gbaud. ONUs and OLT share their own keys to generate pseudo-random sequences. The length of the frame is set as 102400 bits, after the bit data is masked by pseudo-random sequence, it enters the distribution matcher and is converted into symbols with non-uniform distribution. The symbols formed by probability are represented by binary labels and combined with LDPC. The generated sequence is mapped to the complex constellation plane of QAM through the modulator, and the HPGS-16QAM signal is obtained. The generated digital encrypted HPGS-16QAM signal is converted from digital to analog by an arbitrary waveform generator (AWG). Then, after being amplified by an electric amplifier (EA), it is injected into Mach-Zehnder modulator (MZM) for intensity modulation, and the generated modulated optical signal is amplified by an SOA and fed into a 20km SSMF for transmission. The wavelength of the laser is 1550 nm, the linewidth is 100 kHz, and the output optical power is 10 dBm. A VOA is used to attenuate the optical signal to adjust the received optical power of ONU. After receiving the signal, ONU uses offline DSP to recover and decrypt the data. Finally, the recovered data is evaluated to determine the achievable rate.

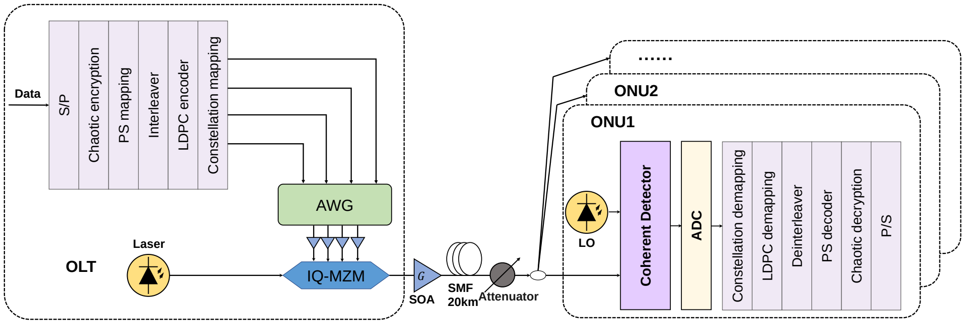

Fig. 4. Simulation setup of PON optimization system based on chaotic encryption and hybrid probability geometric shaping of 16QAM (HPGS-16QAM) signal (AWG: arbitrary waveform generator; MZM: Mach-Zehnder modulator; SOA: semiconductor optical amplifier; LO: local oscillator).

3.2. Simulation results

In this section, simulation results are presented to verify the effectiveness of proposed optimization algorithm. Unless specific stated, we set $K_{max} = 30$, $K_{min} = 10$, $L_{max} = 100$, $L_{min} = 50$, $\beta_s = 2$, $\beta_r = 8$, $\alpha = 30$, $\gamma_{th} = 0.6$, $c = 2$, $n = 30$, $d = 16$, $X_{th} = 3$, $\psi = 0.3$, $G = 2$, $P_{max} = 20$dBm. We compare our proposed algorithm with four benchmarks: 1) Fixed L; 2) Fixed K; 3) Without probability shaping (w/o PS); 4) Without geometric shaping (w/o GS).

Figure 5 illustrates the convergence behavior of the proposed algorithm. It can be observed that after several iterations, the algorithm converges rapidly, indicating its fast convergence speed. Furthermore, the high-speed security objective function value increases from 36.9 to 38.7, demonstrating a significant improvement, which verifies the effectiveness of the algorithm.

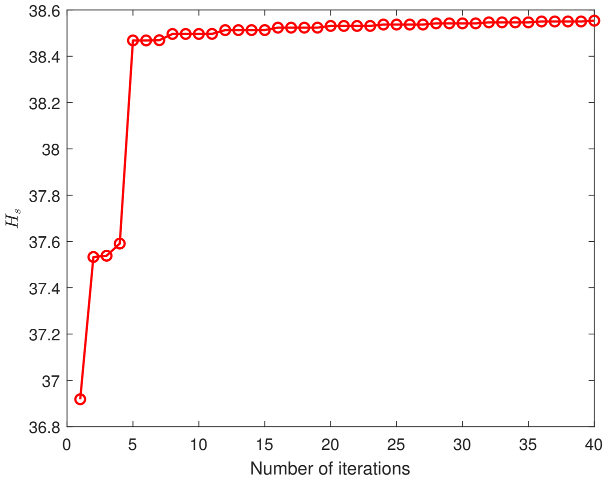

Fig. 5. The curve of the proposed high-speed security objective function H_s and number of iterations.

Figure 6 illustrates the variation of the high-speed security objective function values H_s with respect to the signal-to-noise ratio (SNR). It can be observed that the proposed algorithm achieves the best objective function values within the simulated SNR range, particularly in the low SNR regime. In the high SNR regime, the performance of the proposed algorithm approaches that of the w/o PS and w/o GS schemes, as the rate improvement of PS and GS becomes limited in this region. Notably, the objective function values H_s of the proposed algorithm are significantly higher than those of the comparative algorithms with fixed L and fixed K throughout the entire SNR range. At a SNR of 10 dB, the objective function value of the proposed algorithm exhibits respective improvements of 1.0, 2.6, 4.0, and 4.2 compared to the w/o GS, w/o PS, fixed K, and fixed L schemes.

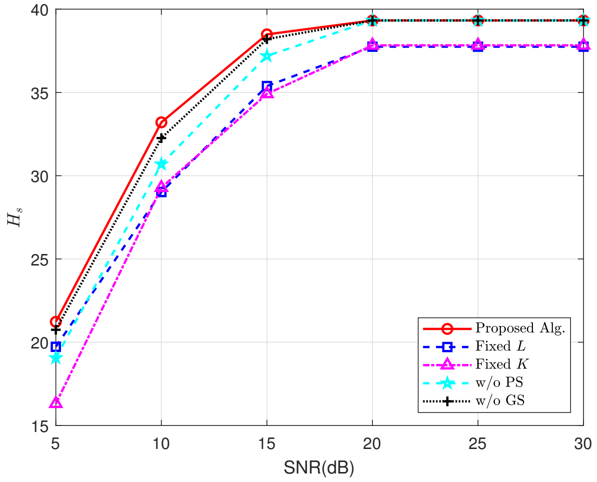

Fig. 6. High-speed security objective function H_s versus SNR for the proposed optimization algorithm, algorithm with fixed L, algorithm with fixed K, algorithm without (w/o) PS and algorithm without (w/o) GS.

Figure 7 illustrates the variation of the minimum Euclidean distance with respect to the SNR. The proposed algorithm exhibits the maximum minimum Euclidean distance in low SNR regions, affirming the efficacy of the proposed algorithm for efficient transmission. As the SNR increases, the minimum Euclidean distance gradually decreases to mitigate the energy consumption associated with system data transmission.

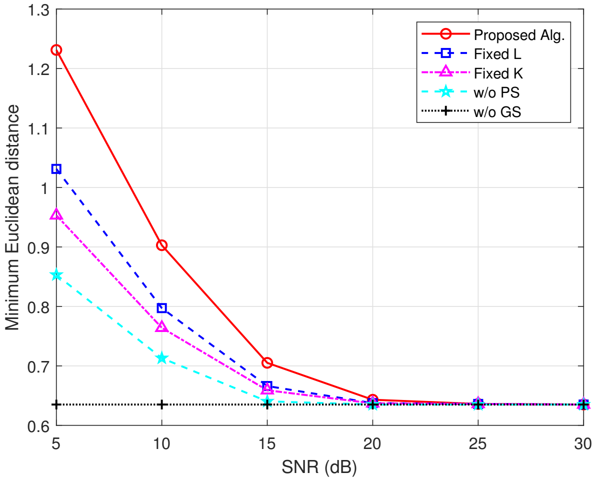

Fig. 7. Minimum Euclidean distance versus SNR for the proposed optimization algorithm, algorithm with fixed L, algorithm with fixed K, algorithm without (w/o) PS and algorithm without (w/o) GS.

Figure 8 illustrates the variation of the bit error rate (BER) with respect to the SNR. The proposed algorithm exhibits superior BER performance in low SNR regions. As the SNR increases, the performance of various optimization algorithms tends to converge. When comparing the proposed algorithm with algorithms that without GS, there is a 2.3 dB improvement in performance at a BER level of 1×10^{-3}.

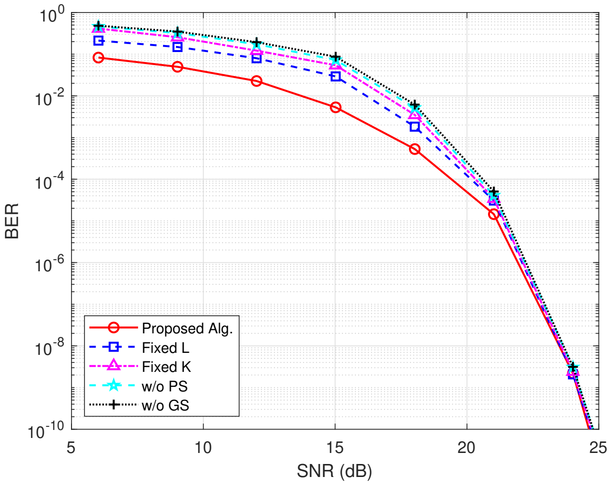

Fig. 8. BER versus SNR for the proposed optimization algorithm, algorithm with fixed L, algorithm with fixed K, algorithm without (w/o) PS and algorithm without (w/o) GS.

Table 1 illustrates the optimized constellation coordinates at an SNR of 15dB. In contrast to the direct design approach outlined in [32], the GS optimization algorithm proposed in this paper aims at maximizing the generalized mutual information. Employing a nonlinear constrained optimization algorithm, it shapes the position coordinates of constellation points, resulting in an optimized coordinate map with irregular geometric shapes. Utilizing the optimization method based on an objective function not only enables the identification of a GS constellation resilient to adverse channel conditions through iterations but also aligns common optimization goals with various parameters, such as probability shaping, fostering a collaborative optimization effect.

Table 1. The coordinates of the optimized GS constellation, when SNR = 15dB.

Constellation Point Index	Optimized Coordinate	Constellation Point Index	Optimized Coordinate
1	-0.9806+1.0751i	9	0.9787+1.0425i
2	-0.9574+0.2614i	10	1.0767+0.3033i
3	-1.1111-0.3935i	11	1.008-0.3225i
4	-1.0718-1.1016i	12	1.077-0.9950i
5	-0.2842-0.9857i	13	0.3335-1.1042i
6	-0.3463-0.2329i	14	0.4255-0.4526i
7	-0.3009+0.5249i	15	0.4956+0.2626i
8	-0.2752+1.1410i	16	0.4617+1.0224i

Figure 9 illustrates the variation of the transmission probabilities of the optimized constellation points for the proposed algorithm with respect to SNR. It can be observed that as SNR increases, the probabilities of all constellation points gradually converge to equal probabilities. This indicates that significant rate gains can be achieved through PS in the low SNR region, while in the high SNR region, equal probability transmission of the constellation points is sufficient.

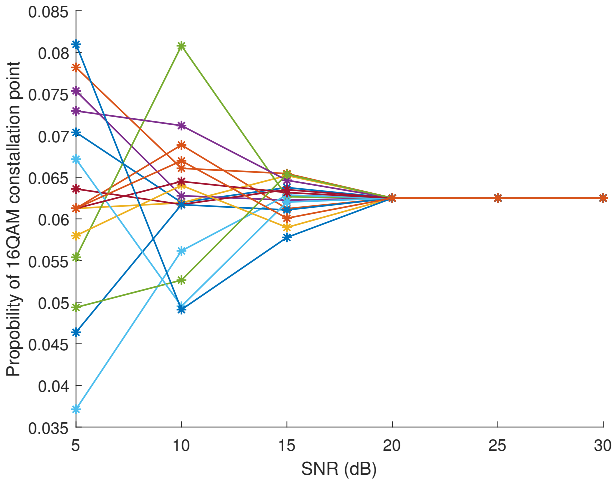

Fig. 9. Symbolic probability of 16QAM probability shaping constellation points versus SNR.

Figure 10 presents the variation of the PS rate $R_s = H(X)/m$ with respect to SNR. It can be observed that the proposed algorithm achieves the maximum PS rate, particularly in the low SNR regime. As SNR increases, the PS rates of all algorithms converge to 1. This analysis demonstrates that the proposed algorithm can yield significant gains in the low SNR region.

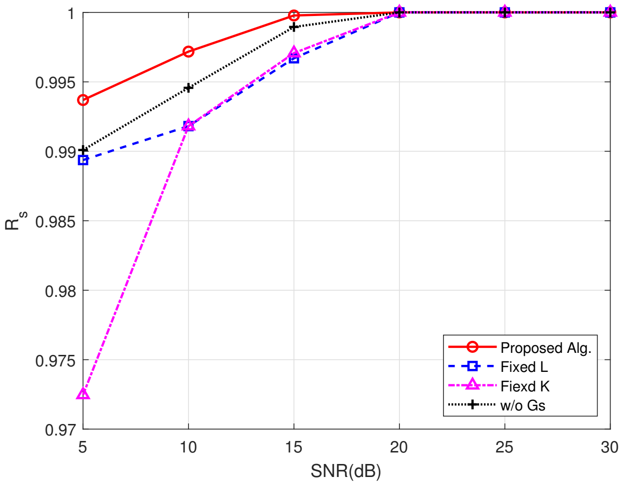

Fig. 10. Probability shaping rate versus SNR.

Figure 11 depicts the variation of the high-speed security objective function values H_s with respect to the minimum key length K_{min}. It can be observed that as the minimum key length increases, the objective function values H_s of all algorithms gradually decrease. The fixed L algorithm exhibits a smaller decrease due to the minimal impact of K variation on the objective function values when L is large. This indicates that, under the given parameter configuration, increasing the key length may result in an increase in encryption complexity that outweighs the improvement in security, leading to a decrease in the objective function. However, the proposed algorithm still outperforms the other comparative algorithms by a significant margin.

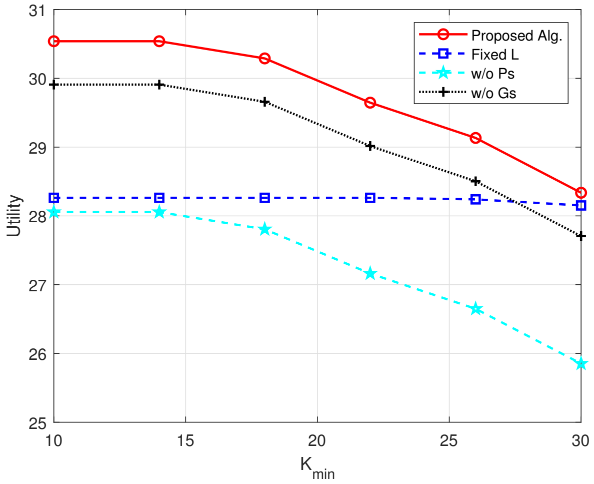

Fig. 11. High-speed security objective function H_s versus minimum key length K_{min} for the proposed optimization algorithm, algorithm with fixed L, algorithm without (w/o) PS and algorithm without (w/o) GS.

Figure 12 illustrates the variation of the high-speed security objective function values H_s with respect to the minimum frame length L_{min}. It can be observed that the objective function values decrease as the minimum frame length increases (except for the fixed K algorithm, which initially increases and then decreases). This is mainly due to the reduction in encryption sensitivity and efficiency as the minimum frame length increases, resulting in a decrease in the objective function. The optimization of all variables in the proposed algorithm significantly outperforms other algorithms, validating the effectiveness of the algorithm.

To show the security performance of the proposed scheme, decryption comparisons are conducted between legal ONUs and illegal ONUs. Figure 13 illustrates the BER curves for different ONUs in the PON system. The received signal at ONU1 is the encrypted signal optimized by the proposed high-speed and secure joint optimization algorithm, featuring identical chaotic mapping parameters and initial values as the OLT. The received signal at ONU2, designated as the legal receiver, consists of only the modulation-optimized non-encrypted signal. The illegal ONU, acting as an eavesdropper, employs a modified Chebyshev map with an initial value $U_1^{'}$ differing from that of ONU1 U_1 by 10^{-16}. From Fig. 13, it is evident that the BER curves for the encrypted ONU1 and the non-encrypted ONU2 are nearly identical, indicating that data encryption does not adversely affect transmission performance. The BER for the legitimate receiver ONU1 gradually decreases with increasing SNR. In contrast, the BER for the illegal ONU remains around 0.5 across all SNR levels, underscoring the efficacy of the proposed high-speed secure optimization algorithm in safeguarding data transmission. The inability to successfully decrypt under a key difference of 10^{-16} demonstrates the key sensitivity of the proposed high-speed secure optimization algorithm.

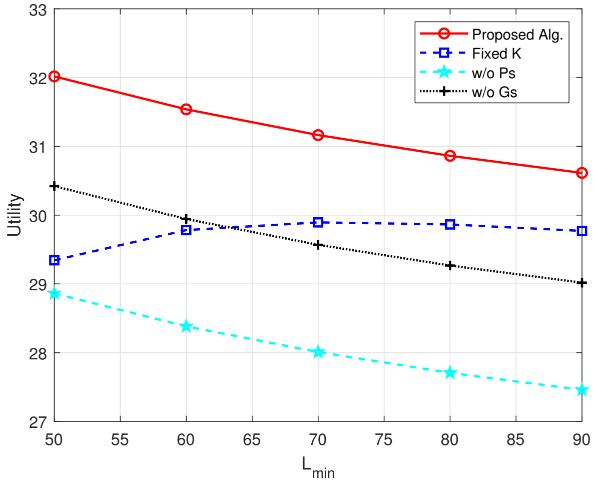

Fig. 12. High-speed security objective function H_s versus minimum frame length L_{min} for the proposed optimization algorithm, algorithm with fixed K, algorithm without (w/o) PS and algorithm without (w/o) GS.

3.3. Security performance

Furthermore, the key space is also a crucial parameter for measuring the security of encryption algorithms. In the cross-mapping chaos illustrated in Fig. 2, the modified Chebyshev map and modified Logistic map are employed as the encryption sequence generators. The parameters μ_1 and μ_2 of the modified Chebyshev map are in the range (0, 10], with a variation step of 10^{-16}, resulting in $S_{\mu_1\mu_2} = 1 \times 10^{34}$. The initial value U_1 of the modified Chebyshev map is within the interval [0, 1], with a variation step of 10^{-16}, yielding $S_{U_1} = 1 \times 10^{16}$. The initial value X_1 of the modified Logistic map is in the range (0, 1), with a variation step of 10^{-16}, leading to $S_{X_1} = 1 \times 10^{16}$. Consequently, the key space of the encryption algorithm in this paper is $S = S_{\mu_1\mu_2} S_{U_1} S_{X_1} = 1 \times 10^{66}$.

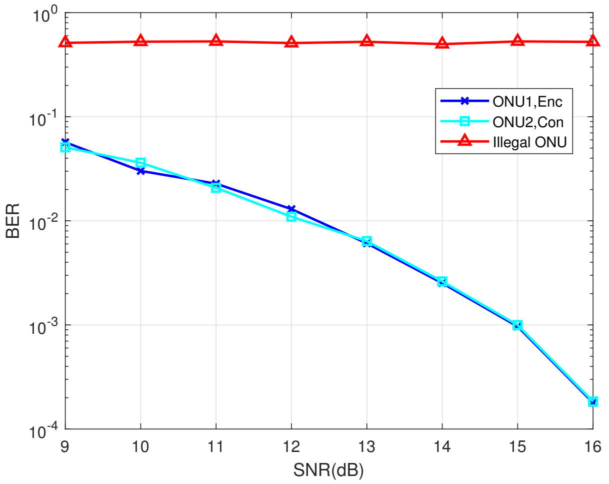

Fig. 13. BER versus SNR under different security scenarios.

Table 2 displays the key spaces of typical high-speed secure encryption schemes in PON. A larger key space implies higher security. However, a larger key space often requires more complex computations and key management. The chaos cross-mapping scheme presented in this paper can be expanded by incorporating more one-dimensional chaos. Nevertheless, considering the complexity of encryption and the system performance overhead, we did not deliberately increase the key space since $1 \times 10^{66} > 2^{100}$ [38], which is already sufficient to withstand brute-force attacks.

Table 2. Scheme Comparison Analysis

Schemes	Proposed	[25]	[30]	[31]	[39]
Key space	1×10^{66}	3×10^{76}	6.4×10^{91}	1×10^{120}	1.98×10^{73}

4. Conclusion

To solve the problem that the existing optical access network lacks the standard to evaluate the rate and security, this paper takes PON as an example, proposes a high-speed and security joint optimization scheme of optical access network based on convex optimization, and jointly optimizes the frame length, key length, PS and GS to constructs a security optimization objective function U_s, the high-speed optimization objective function GMI and a high-speed and security joint optimization objective function H_s measuring the security and quality of the communication. Firstly, we described the system architecture of optical access networks and provide quantitative metrics for rate and security. Then, based on these metrics, we formulated an optimization problem with constraints, including maximum power constraint, probability and constraint, amplifier performance constraint, minimum threshold constraint for NGMI, as well as key and frame length constraints. The constructed problem is nonlinear and non-convex, with highly coupled optimization variables. Finally, we employed an alternating optimization algorithm to decompose the optimization into four sub-problems, and then utilize algorithms such as SCA and DC to transform the non-convex sub-problems into convex optimization problems for iterative solving. The experimental results demonstrate that the high-speed and security objective function value of the joint optimization scheme is obviously enhanced, thus verifying the effectiveness of the optical access network high-speed and security joint optimization algorithm based on convex optimization.

In the future, this high-speed and security joint optimization scheme can be extended wide-area networks or metropolitan area networks or large-scale local area networks. Different quantitative metrics of rate and security can be given according to different network encryption algorithms and high-speed schemes to establish high-speed and security joint optimization models.

Funding. Chongqing Postdoctoral Funding Project (2112012727685993); China Postdoctoral Science Foundation (2021M700563); Chongqing Municipal Education Commission (CXQT21019, KJQN202100643); National Natural Science Foundation of China (62025105, 62071076, 62205043).

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. H. S. Abbas and M. A. Gregory, "The next generation of passive optical networks: A review," J. Netw. Comput. Appl. **67**, 53–74 (2016).
2. Y. Zhu, L. Yi, B. Yang, *et al.*, "Comparative study of cost-effective coherent and direct detection schemes for 100 Gb/s/λ PON," J. Opt. Commun. Netw. **12**(9), D36–D47 (2020).
3. J. Zhang, J. Yu, X. Li, *et al.*, "200 gbit/s/λ pdm-pam-4 pon system based on intensity modulation and coherent detection," J. Opt. Commun. Netw. **12**(1), A1–A8 (2020).
4. I. B. Kovacs, M. S. Faruk, and S. J. Savory, "200 gb/s/λ upstream pon using polarization multiplexed pam4 with coherent detection," IEEE Photonics Technol. Lett. **35**(18), 1014–1017 (2023).
5. N. Deng, L. Zong, H. Jiang, *et al.*, "Challenges and enabling technologies for multi-band wdm optical networks," J. Lightwave Technol. **40**(11), 3385–3394 (2022).
6. L. Zhou, H. He, Y. Zhang, *et al.*, "Enhancement of spectral efficiency and power budget in wdn-pon employing ldpc-coded probabilistic shaping pam8," IEEE Access **8**, 45766–45773 (2020).
7. M. P. Yankov, F. Da Ros, E. P. da Silva, *et al.*, "Constellation shaping for wdm systems using 256qam/1024qam with probabilistic optimization," J. Lightwave Technol. **34**(22), 5146–5156 (2016).
8. A. Matsushita, M. Nakamura, F. Hamaoka, *et al.*, "High-spectral-efficiency 600-gbps/carrier transmission using pdm-256qam format," J. Lightwave Technol. **37**(2), 470–476 (2018).
9. V. E. Houtsma and D. T. van Veen, "Investigation of modulation schemes for flexible line-rate high-speed TDM-PON," J. Lightwave Technol. **38**, 3261–3267 (2020).
10. D. Zou and I. B. Djordjevic, "Bit loading-based irregular LDPC coded-modulation for high-speed optical communications," *Int. Conf. Trans. Opt. Netw. (ICTON)*, (IEEE, 2016), pp. 1–4.
11. D. Zou and I. B. Djordjevic, "FPGA-based rate-compatible LDPC codes for the next generation of optical transmission systems," IEEE Photonics J. **8**(5), 1–8 (2016).
12. X. Sun, M. Yang, and I. B. Djordjevic, "Real-time FPGA-based rate adaptive LDPC coding for data center networks and PONs," in *Eur. Conf. Opt. Commun. (ECOC)*, (IEEE, 2018), pp. 1–3.
13. I. B. Djordjevic, "On advanced FEC and coded modulation for ultra-high-speed optical transmission," IEEE Commun. Surv. Tutor. **18**(3), 1920–1951 (2016).
14. F. R. Kschischang and S. Pasupathy, "Optimal nonuniform signaling for Gaussian channels," IEEE Trans. Inf. Theory **39**(3), 913–929 (1993).
15. S. Baur and G. Böcherer, "Arithmetic distribution matching," in *Int. ITG Conf. Syst. Commun. Coding*, (VDE, 2015), pp. 1–6.
16. P. Schulte and G. Böcherer, "Constant composition distribution matching," IEEE Trans. Inf. Theory **62**(1), 430–434 (2015).
17. A. Amari, S. Goossens, Y. C. Gültekin, *et al.*, "Introducing enumerative sphere shaping for optical communication systems with short blocklengths," J. Lightwave Technol. **37**(23), 5926–5936 (2019).
18. M. Fu, Q. Liu, Y. Xu, *et al.*, "Multi-dimensional distribution matching with bit-level shaping for probabilistically shaped high order modulation formats," J. Lightwave Technol. **40**(9), 2870–2879 (2022).
19. G. Böcherer, F. Steiner, and P. Schulte, "Bandwidth efficient and rate-matched low-density parity-check coded modulation," IEEE Trans. Commun. **63**(12), 4651–4665 (2015).
20. G. Böcherer, P. Schulte, and F. Steiner, "Probabilistic shaping and forward error correction for fiber-optic communication systems," J. Lightwave Technol. **37**(2), 230–244 (2019).
21. J. Cho and P. J. Winzer, "Probabilistic constellation shaping for optical fiber communications," J. Lightwave Technol. **37**(6), 1590–1607 (2019).
22. J. Cho, "Balancing probabilistic shaping and forward error correction for optimal system performance," in *Opt. Fiber Commun. Conf.*, (Optica Publishing Group, 2018), pp. M3C–2.
23. R. Zhang, N. Kaneda, Y. Lefevre, *et al.*, "Probabilistic and geometric shaping for next-generation 100G flexible PON," in *Eur. Conf. Opt. Commun. (ECOC)*, (IEEE, 2020), pp. 1–4.

24. M. Baptista, "Cryptography with chaos," Phys. Lett. A **240**(1-2), 50–54 (1998).
25. Z. Zhang, Y. Luo, C. Zhang, *et al.*, "Constellation shaping chaotic encryption scheme with controllable statistical distribution for OFDM-PON," J. Lightwave Technol. **40**(1), 14–23 (2022).
26. X. Xu, B. Liu, X. Wu, *et al.*, "A robust probabilistic shaping PON based on symbol-level labeling and rhombus-shaped modulation," Opt. Express **26**(20), 26576–26589 (2018).
27. J. Zhao, B. Liu, Y. Mao, *et al.*, "High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization," Opt. Express **28**(14), 21236–21246 (2020).
28. C. Zhang, Y. Yan, T. Wu, *et al.*, "Phase masking and time-frequency chaotic encryption for DFMA-PON," IEEE Photonics J. **10**(4), 1–9 (2018).
29. Z. Hu and C.-K. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON," J. Lightwave Technol. **36**(16), 3373–3381 (2018).
30. X. Liang, C. Zhang, Y. Luo, *et al.*, "Secure encryption and key management for OFDM-PON based on chaotic Hilbert motion," J. Lightwave Technol. **41**(6), 1619–1625 (2022).
31. Y. Luo, C. Zhang, X. Liang, *et al.*, "Secure OFDM-PON using three-dimensional selective probabilistic shaping and chaos," Opt. Express **30**(14), 25339–25355 (2022).
32. W. Zeng, C. Zhang, X. Liang, *et al.*, "Chaotic phase noise-like encryption based on geometric shaping for coherent data center interconnections," Opt. Express **32**(2), 1595–1608 (2024).
33. A. Alvarado, T. Fehenberger, B. Chen, *et al.*, "Achievable information rates for fiber optics: Applications and computations," J. Lightwave Technol. **36**(2), 424–439 (2018).
34. J. Cho, L. Schmalen, and P. J. Winzer, "Normalized generalized mutual information as a forward error correction threshold for probabilistically shaped QAM," in *Eur. Conf. Opt. Commun.* (ECOC), (2017), pp. 1–3.
35. A. Hu, X. Gong, and L. Guo, "Joint encryption model based on a randomized autoencoder neural network and coupled chaos mapping," Entropy **25**(8), 1153 (2023).
36. M. Haleem, C. Mathur, R. Chandramouli, *et al.*, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," IEEE Trans. Depend. Secur. Comput. **4**(4), 313–324 (2007).
37. M. Razaviyayn, "Successive convex approximation: Analysis and applications," Ph.D. thesis (2014).
38. G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurcation Chaos **16**(08), 2129–2151 (2006).
39. J. Ren, B. Liu, D. Zhao, *et al.*, "Chaotic constant composition distribution matching for physical layer security in a PS-OFDM-PON," Opt. Express **28**(26), 39266–39276 (2020).