A Simple Chaotic Encryption Scheme for Probabilistically Shaped Transmissions

A Simple Chaotic Encryption Scheme for Probabilistically Shaped Transmissions

Yu Gu[1,2], Gabriella Bosco[2], Feng Tian[1], and Dario Pilori[2]

1. Beijing University of Posts and Telecommunications, 100876, Beijing, China
2. Politecnico di Torino, 10129, Torino, Italy
yu.gu@polito.it

***Abstract*—We propose a simple encryption scheme that preserves the probability distribution of constellation symbols, ensuring seamless integration into communication systems employing probabilistic shaping, while enhancing security performance.**

Keywords—probabilistic amplitude shaping, distribution matcher, chaotic encryption

I. INTRODUCTION

The advancement of optical communications necessitates the reinforcement of security measures within optical communication systems to thwart unauthorized breaches. The chaotic systems are extensively utilized in physical-layer encryption owing to their heightened initial sensitivity, excellent pseudo-random characteristics, and unpredictability. Encryption protocols employing chaotic systems exhibit enhanced confidentiality and robust resistance against decryption attempts [1]. In [2], a pioneering security mechanism employing chaotic constellation shifting is deployed to bolster the physical-layer security of optical networks. A symbol-level encryption scheme based on phase ambiguity was introduced in [3], which effectively preserves the shaping benefits given by probabilistic constellation shaping (PCS) and mitigates error convergence in blind equalizers. Existing encryption schemes suffer from inherent drawbacks, including elevated encryption costs and performance degradation during transmission. Hence, there exists a pressing need to develop a novel encryption scheme characterized by simplified encryption procedures while retaining the shaping advantages associated with probability shaping techniques.

In this paper, our focus is on devising a cost-effective encryption scheme that preserves shaping advantages. We propose a method based on the probabilistic amplitude shaping (PAS) algorithm. Initially, constellation points are generated following the Maxwell-Boltzmann (MB) distribution. Subsequently, chaotic elements are introduced within the Low Density Parity-check Code (LDPC) encoding segment, ensuring that the overall probability distribution remains unchanged. Simulation results demonstrate that our proposed scheme effectively ensures security with reduced complexity while maintaining transmission performance.

II. PRINCIPLES OF THE ENCRYPTION SCHEME BASED ON PROBABILISTIC AMPLITUDE SHAPING

The system step includes a Distribution Matcher (DM) converting uniformly distributed information bits of the LDPC codewords into positive amplitudes of *M*-PAM symbols, aligning with the MB distribution. A binary systematic Forward Error Correction (FEC) encoder generates parity bits, distributed uniformly between {0,1}. These parity bits, or uncoded uniform bits, exclusively serve to set the sign of amplitude symbols in each dimension [4]. To maintain the probability distribution established by the DM, a scheme utilizing a three-dimensional (3D) Jerk chaotic system [5] is introduced to encrypt the parity bits during the FEC encoding process. The inclusion of the proposed encryption scheme in the probabilistically shaped transmission is illustrated in Fig.1.

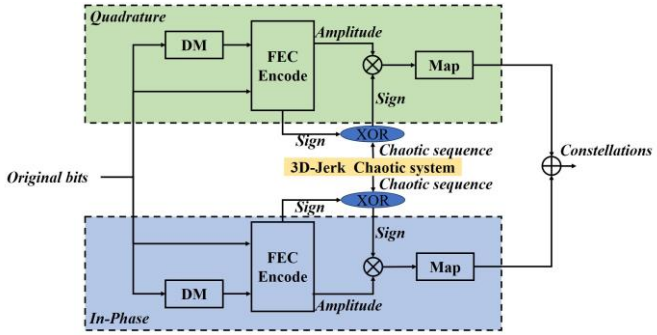


Fig. 1. The proposed scheme diagram of the encryption.

In this scheme, two chaotic sequences of the 3D-Jerk chaotic system [5] are used in the encryption process. The phase diagram of 3D-Jerk chaotic system is shown in Fig.2(a). The distribution of the chaotic sequence p_i and q_i on the phase plane is shown in Fig.2(b). The input PRBS sequences P_{Ii} and P_{Qi} are transformed accordingly to the following equations:

$$P'_{Ii} = xor(P_{Ii}, w_{Ii}) \quad (2)$$

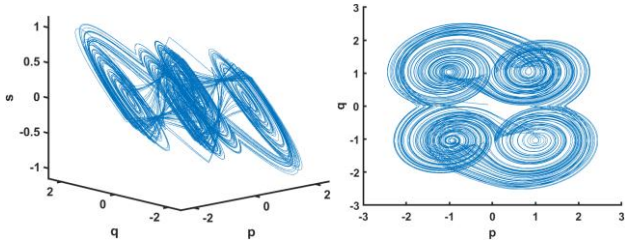
$$P'_{Qi} = xor(P_{Qi}, w_{Qi}) \quad (3)$$

$$w_{Ii} = floor(mod(p_i * 1e14,2)) \quad (4)$$

$$w_{Qi} = floor(mod(q_i * 1e14,2)) \quad (5)$$

where $floor(\cdot)$ is the rounding down operation. w_{Ii} and w_{Qi} are chaotic bit sequences used in the XOR operations. P'_{Ii} and

P'_{Qi} are the encrypted bit sequences to be mapped into sign symbol {-1, +1}. In this scheme, chaotic sequence $\{p_i\}$ and $\{q_i\}$ change very slowly. Eq. (4), (5) can generate random {0,1} bit sequences $\{w_{Ii}\}$ and $\{w_{Qi}\}$ to ensure encryption effectiveness, as shown in Fig3. (a)-(d).



(a) (b)

Fig. 2. (a) Phase diagram of 3D-Jerk chaotic system (b) The chaotic sequences p and q on the phase plane.

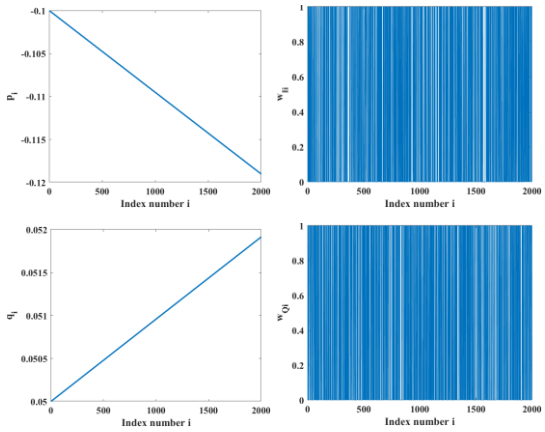


Fig. 3. (a) (b) (c) (d) Time domain diagram of p_i, q_i, w_{Ii} and w_{Qi}.

III. Results and Discussions

A. Generalized Mutual Information (GMI)

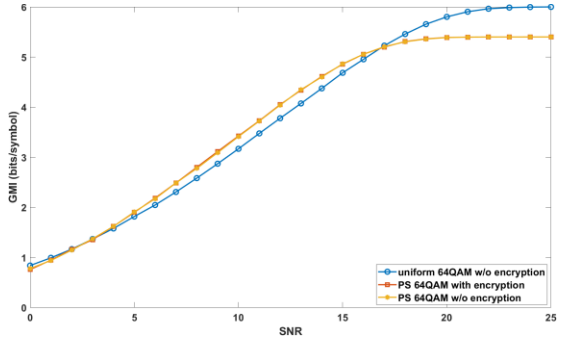


Fig. 4. Simulation results of GMI performance.

In this paper, the performance of the proposed scheme is assessed through numerical simulations in terms of the Generalized Mutual Information (GMI), which is a universal and efficient metric for comparing various modulation formats, in the presence of soft-decision FEC [6]. Fig.4 illustrates the GMI for three different modulation formats. Remarkably, the GMI curves of PS-64QAM with and without encryption closely overlap. This observation suggests that the distribution of the encrypted signal remains consistent with the original MB distribution.

B. BER performance

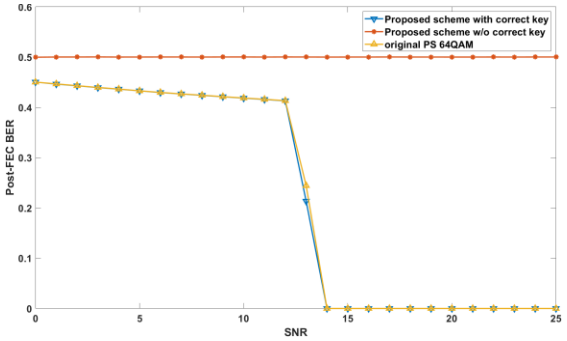


Fig. 5. The simulated post-FEC BER performance.

Fig.5 illustrates the simulated post-FEC BER performance, utilizing DVB-S2 irregular binary LDPC codes with a block length of 64800 and a code rate of 4/5. The results demonstrate that the BER of the proposed encryption scheme remains constant at 0.5 across varying SNRs, indicating the consistent and reliable encryption effectiveness of the scheme in the absence of the correct key. The curves representing the original PS 64QAM and the proposed encryption scheme with the correct key exhibit close alignment, suggesting that the encryption scheme successfully maintains the performance advantages provided by probability shaping techniques.

IV. Conclusions

In this paper, we introduce a simple novel chaotic encryption scheme combined with probabilistic amplitude shaping. This scheme enhances the security of the signal without reducing transmission performance.

Acknowledgment

This work was supported by CSC; National Key R&D program of China (2020YFB1805805); National Natural Science Foundation of China (NSFC) (62021005, 62027819).

References

[1] M. Bi, X. Fu, X. Zhou, L. Zhang, G. Yang, X. Yang, S. Xiao and W. Hu, "A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON," *IEEE Photonics Journal*, vol. 9, no. 1, pp. 1-10, 2017.

[2] A. Sultan. X. Yang, A. A. E. Hajomer, and W. Hu, "Chaotic Constellation Mapping for Physical-Layer Data Encryption in OFDM-PON," *IEEE Photonics Technology Letters*, vol. 30, no. 4, pp. 339-342, 2018.

[3] X. Wang, Z. Li, Q. Zhang, X. Pan, R. Gao, X. Xin, H. Yao, F. Tian, Q. Tian and Y. Wang, "Chaotic physical layer encryption scheme based on phase ambiguity for a DMT system," *Optics Express*, vol. 30, no. 9, pp.14782-14797, 2022.

[4] F. Buchali, F. Steiner, G. Böcherer, L. Schmalen, P. Schulte, and W. Idler, "Rate adaptation and reach increase by probabilistically shaped64-QAM: An experimental demonstration," *Journal of Lightwave Technology*, vol. 34, no. 7, pp. 1599-1609, Apr. 2016.

[5] F. Wang, B. Zhu, K. Wang, M. Zhao, L. Zhao, and J. Yu, "Physical Layer Encryption in DMT Based on Digital Multi-Scroll Chaotic System," *IEEE Photonics Technology Letters*, vol. 32, no. 20, pp. 1303-1306, 2020.

[6] S. Zhang and F. Yaman, "Design and comparison of advanced modulation formats based on generalized mutual information," *Journal of Lightwave Technology*, vol. 36, no. 2, pp. 416-423, 2017.