Physical Layer Encryption Scheme Based on Dynamic Constellation Rotation

Yujie Hou*, Guyue Li*†, Shuping Dang‡, Lei Hu*, Aiqun Hu†‖
*School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China
†Purple Mountain Laboratories for Network and Communication Security, Nanjing, 210096, China
‖National Mobile Communications Research Laboratory, Southeast University, Nanjing, 210096, China
‡Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, United Kingdom
Corresponding author: Guyue Li, Email: guyuelee@seu.edu.cn

***Abstract*—Physical layer encryption (PLE) has emerged as a promising technique to secure wireless communications. Different from conventional cryptography implemented at higher layers, PLE exploits the randomness of wireless channels to adjust symbol patterns at the physical layer, by which both data and modulation information can be protected. However, existing PLE schemes face challenges of security and robustness in practical usage. In a slowly varying environment, the constellation variation is negligible, which results in the vulnerability of PLE to the differential attack. Moreover, the decryption error rate of PLE is high when the channel reciprocity is not ideal. To tackle these problems, we exploit data randomness to enhance the dynamics of constellation variations between adjacent frames. Then we utilize analog-based encryption instead of digital-based encryption to dynamically rotate constellation, which reduces quantization loss and improves robustness to channel phase errors. Simulation results verify that the proposed scheme can effectively resist the differential attack and provide approximately a 4.5 dB gain when the bit error ratio (BER) is 0.001.**

***Index Terms*—Physical layer encryption, symbol patterns, differential attack, data randomness, constellation rotation.**

I. Introduction

Security is always a serious issue for wireless communication systems due to the broadcast nature of the wireless channel. The security of traditional wireless communication relies mainly on upper layer encryption mechanisms. However, it can only protect the data content without protecting its modulation information. A traffic analysis attacker can intercept transmitted signals and study their external characteristics to obtain information about the operation of a communication system [1]. Moreover, it is challenging to generate and distribute keys to devices with limited resources. Therefore, a more secure and lightweight encryption scheme is needed to secure wireless communications.

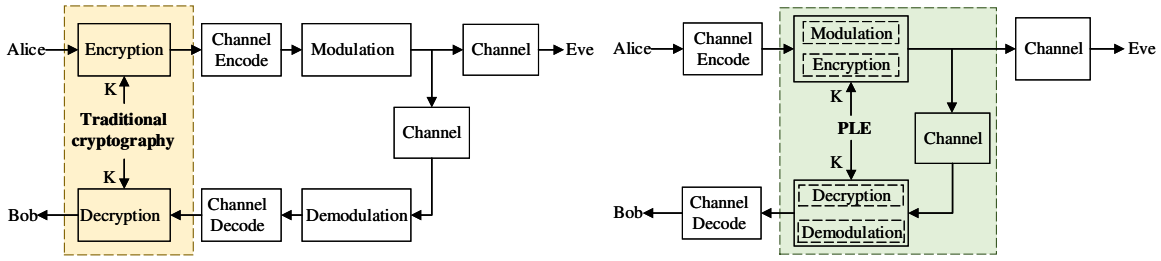
Physical layer encryption (PLE) is an effective technique to enhance the security of wireless transmission [2, 3]. As shown in Fig. 1, unlike traditional upper layer cryptography, the encryption of PLE is added after channel coding or modulation. Based on the generation of shared physical layer keys, PLE aims to design signal constellations to protect the modulation symbols without leaking modulation information. The design of the constellation patterns provides a large key space and is also effective in resisting traffic analysis attacks. Moreover, PLE is of low complexity and overhead and enables using lightweight transmission schemes, which are suitable for resource-limited Internet-of-Things (IoT) applications.

Most PLE schemes can be divided into the categories of post-modulation encryption and pre-modulation encryption. Post-modulation encryption schemes are based on encryption of the modulated symbols, exploiting the effects of channel and noise to provide security. The main methods used in these PLE schemes are constellation rotation [4, 5], amplitude adjustment [6], subcarrier obfuscation [7, 8], and symbol blurring [9], by which eavesdroppers cannot identify the new constellation pattern and fail to obtain private information. Pre-modulation encryption schemes are always based on conventional encryption, namely stream cipher encryption, making use of bitwise exclusive OR (XOR) operation to generate one ciphertext bit [10]. Besides, to enhance the key space and the key sensitivity of PLE schemes, chaotic systems are introduced into these schemes for joint design because of their special characteristics of pseudo randomness, ergodicity, and high sensitivity to initial values [11, 12].

However, the aforementioned PLE schemes do not consider the impact of weak channel randomness and vulnerabilities under various attacks in a slowly varying environment [13]. Moreover, the pilot symbol is conveyed in plaintext. As a consequence, an eavesdropper can explore the relationship of adjacent frames to conduct a differential attack. Furthermore, some existing PLE approaches are based on the assumption that legitimate communicating parties have perfect channel reciprocity or predefined key seeds, which is not always true in practical usage. The reliability of these PLE schemes is compromised if their original assumptions do not hold.

To tackle these problems, we propose a PLE scheme based on dynamic constellation rotation (DCR) to achieve both security and reliability. The main contributions of this paper are listed as follows:

- To enhance the randomness and sensitivity of constellation patterns, we propose a method that combines the randomness of data and channels. The generated constellation patterns are dynamically updated for each frame and are resistant to the differential attack.
- We design a PLE scheme to perform dynamic constellation rotation on modulated symbols with unquantized



(a) System model of traditional cryptography. (b) System model of PLE.

Fig. 1. Comparison of the structure between traditional cryptography and PLE.

phase information, which secures modulation information and reduces the quantization loss.

- We conduct simulations and obtain simulation results to show that the bit error ratio (BER) performance of DCR is significantly improved compared to the conventional quantization scheme, with a gain of 4.5 dB when BER is 0.001. This verifies that our proposed scheme is more robust against channel phase errors.

II. PLE Based on Dynamic Constellation Rotation

In this section, we first describe the system model of the PLE scheme and then introduce the proposed DCR scheme and its three main modules, including phase information extraction, dynamic pattern generation, and constellation rotation. The Schematic of the proposed scheme is shown in Fig. 2.

A. PLE System Model

We consider a general PLE model with three communication nodes that operate in the time-division duplex (TDD) mode. All nodes are equipped with a single antenna. Alice and Bob are two legitimate users who attempt to employ reciprocal channel information to generate the secret keys and achieve secure communications. Meanwhile, Eve is a passive eavesdropper who intends to intercept the confidential information transmitted over the legal channel.

The implementation of PLE is based on the generation of shared information, and, therefore, the uplink and downlink channels between Alice and Bob are modeled as complex Gaussian random variables $\mathbf{h}^{AB}(k) \in \mathbb{C}^{N\times 1}$ and $\mathbf{h}^{BA}(k) \in \mathbb{C}^{N\times 1}$, where $\mathbb{C}^{M\times N}$ denotes the space of complex matrices of size $M \times N$; also, k denotes the transmission index, and N is the number of subcarriers. The received signals at Bob and Alice are represented as

$$\mathbf{y}^B(k) = \mathbf{X}(k)^A\mathbf{h}^{AB}(k) + \mathbf{w}^B(k), \tag{1}$$

and

$$\mathbf{y}^A(k) = \mathbf{X}(k)^B\mathbf{h}^{BA}(k) + \mathbf{w}^A(k), \tag{2}$$

where $\mathbf{X}(k) = \mathrm{diag}(x_0(k), x_1(k), \cdots, x_{N-1}(k))$ represents the transmitted orthogonal frequency division multiplexing (OFDM) symbol in the kth frame; $\mathbf{w}(k) \in \mathbb{C}^{N\times 1}$ is the complex additive white Gaussian noise (AWGN) with variance σ_h^2; superscripts A and B represent Alice and Bob respectively. The transmission index starts from $k = 0$ and ends at a frame

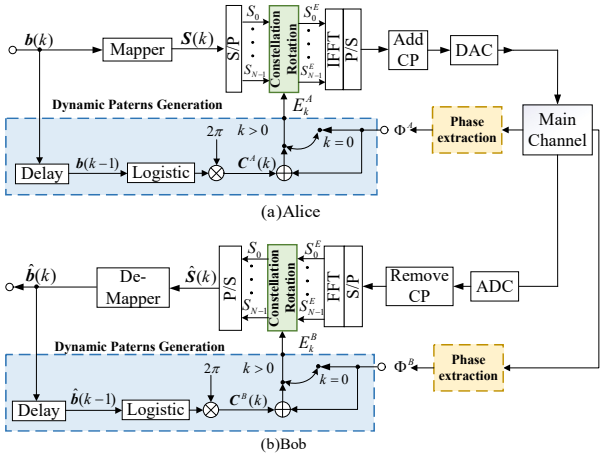


Fig. 2. Schematic of the proposed PLE scheme.

length $k = M$, which restarts from $k = 0$ when the new phase information is extracted from the channel.

According to the channel reciprocity resulted from the TDD mode, Alice and Bob can extract similar channel information within the coherent time. Eve is assumed at least $\lambda/2$ (λ is the carrier wavelength) away from other nodes, at which point the wiretap channel is independent of the legitimate channel.

B. Phase Information Extraction

To enhance security of extracted phases, locally generated random phases are used. At the beginning of phase extraction, Alice generates and sends downlink probing signal $\mathbf{S}^A = \mathrm{diag}(s_0^A, s_1^A, \cdots, s_{N-1}^A)$ to Bob, where $s_i^A = \exp(j\varphi_i^A)$, and φ_i^A is the initial phase randomly generated on a uniform basis over $[0, 2\pi)$, which is only known to Alice. Then the frequency-domain signal $\mathbf{y}^B = [y_0^B, y_1^B, \ldots, y_{N-1}^B]^T$ received by Bob can be written as

$$\begin{aligned} y_i^B &= h_i s_i^A + w_i^B \\ &= |h_i| \exp\left(j\varphi_i^A + \theta_i\right) + w_i^B, \end{aligned} \tag{3}$$

where y_i^B is the frequency-domainn symbol received by Bob, and w_i^B is the additive noise. $h_i = |h_i| \exp(j\theta_i)$ denotes channel response of the ith sub-channel.

Once receiving the downlink probing signal, Bob sends $\mathbf{S}^B = \mathrm{diag}(s_0^B, s_1^B, \cdots, s_{N-1}^B)$ to Alice, where $s_i^B = \exp(j\varphi_i^B)$ and φ_i^B is the initial phase randomly generated on

a uniform basis over $[0, 2\pi)$, which is only known to Bob. To obtain an equivalent phase sequence, Bob estimates the phase of received signal and notes the estimated phase $\varphi_i^A + \theta_i + \varepsilon_i^B$ as $\hat{\varphi}_i^{AB}$, where ε_i^B is the noise component by estimation with variance σ_n^2. Similarly, Alice estimates the phase of received signal and notes the estimated phase $\varphi_i^B + \theta_i + \varepsilon_i^A$ as $\hat{\varphi}_i^{BA}$.

Then, by summing the locally generated random phase sequence and the extracted phase sequence, Bob and Alice can compute the initial phase sequences $\mathbf{\Phi}^B \in \mathbb{C}^{N\times 1}$ and $\mathbf{\Phi}^A \in \mathbb{C}^{N\times 1}$ as

$$\Phi_i^B = \hat{\varphi}_i^{AB} + \varphi_i^B \bmod 2\pi, \tag{4}$$

and

$$\Phi_i^A = \hat{\varphi}_i^{BA} + \varphi_i^A \bmod 2\pi. \tag{5}$$

Considering the influence of non-reciprocal factors, there will be a certain difference between $\mathbf{\Phi}^A$ and $\mathbf{\Phi}^B$. To discuss the influence of channel phase error, the error between the extracted phase sequence can be quantified as

$$\boldsymbol{\varepsilon} = \mathbf{\Phi}^B - \mathbf{\Phi}^A, \tag{6}$$

where the each element in $\boldsymbol{\varepsilon} \in \mathbb{C}^{N\times 1}$ is modeled as a uniformly distributed random variable in the interval $[-\Delta, +\Delta]$ and Δ is the maximum phase error of the channel.

Conventional PLE schemes normally perform multiple rounds of channel detection and quantify the extracted phase information for encryption. However, in a static environment, the generated keys suffer from a lack of randomness, which require additional mechanisms to enhance security and secrecy.

C. Dynamic Pattern Generation

The dynamics of the constellations in our proposed scheme are derived from the data and chaotic sequences. We utilize data-based chaotic sequences to enhance the variation of the extracted phase information per frame. Specifically, after the extraction of phase sequences, the binary sequences $\{b_n(k-1)\}_{n=0}^{L-1}(k \geq 1)$ are transformed into a decimal number $x_0^A(k)$ to dertermine the initial seed of chaotic sequence:

$$x_0^A(k) = \sum_{n=0}^{L-1} b_n(k-1) \cdot 2^{-n}, \tag{7}$$

where $b_n(k-1)$ represents the nth bit of the $(k-1)$th frame, and L is the number of bits. For the convenience of explanation and mathematical analysis, the logistic map given by:

$$x_{n+1} = 4x_n(1 - x_n), \tag{8}$$

is used. When the initial value satisfies $0 < x_0 < 1$, the logistic mapping is said to be in a chaotic state. We take x_0^A as the initial value and iterate $I + N - 1$ times to generate a chaotic sequence $\mathbf{C}^A(k) \in \mathbb{C}^{N\times 1}$, which is then mapped linearly to the interval $(0, 2\pi)$ as follows:

$$\mathbf{C}^A(k) = 2\pi\left[x_I^A(k), x_{I+1}^A(k), \ldots, x_{I+N-1}^A(k)\right]. \tag{9}$$

Finally, a dynamic sequence is generated by

$$\mathbf{E}^A(k) = \begin{cases} \mathbf{C}^A(k) + \mathbf{\Phi}^A, 0 < k \leq M, \\ \mathbf{\Phi}^A \qquad\quad , k = 0. \end{cases} \tag{10}$$

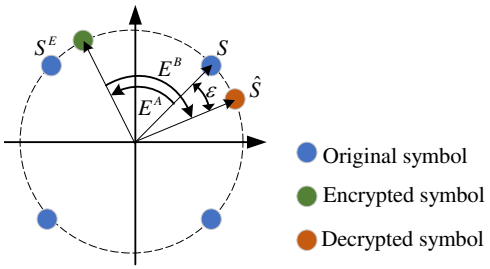


Fig. 3. Constellation rotation and reverse rotation(QPSK).

The same operations are performed at Bob to generate a similar dynamic sequence $\mathbf{E}^B(k)$. From (10), it can be seen that even though $\mathbf{\Phi}^A$ remains constant, the difference of transmitted data per frame can still vary $\mathbf{C}^A(k)$, resulting in $\mathbf{E}^A(k)$ to be highly dynamic.

D. Random Constellation Rotation

To make the legitimate end recover the received bits as correctly as possible, we design an encryption method based on random constellation rotation. The constellation rotation and inverse rotation under quadrature phase shift keying (QPSK) are shown in Fig. 3. In particular, bit sequence $\mathbf{b}$ at Alice is mapped to N parallel modulation symbols from the symbol constellation. The kth symbol is denoted by S_k, where $k = 0, 1, ..., N-1$. After performing the serial-to-parallel conversion to the original OFDM symbol $\mathbf{S} = (S_0, S_1, \ldots, S_{N-1})$, modulation symbols are encrypted by constellation rotation

$$\mathbf{S}^E = \mathbf{D}_A \mathbf{S}^T, \tag{11}$$

where $\mathbf{D}_A = \mathrm{diag}(e^{jE_0^A}, e^{jE_1^A}, \cdots, e^{jE_{N-1}^A})$ is a phase rotation matrix, and $\mathbf{S}^E = \left(S_0^E, S_1^E, \ldots S_N^E\right)^T$ is the substitution of original OFDM symbols. Then $\mathbf{S}^E$ are transformed into time-domain symbols through inverse fast Fourier transform (IFFT), which are loaded on the carrier and transmitted after parallel-to-serial conversion, cyclic prefix (CP) and pilot insertion.

As shown in Fig. 2 (b), Bob performs the reverse process of Alice's operations to obtain the encrypted OFDM symbols $\mathbf{S}^E$ and perform inverse rotation decryption in order to recover the modulated symbols by

$$\hat{\mathbf{S}} = \mathbf{D}_B \mathbf{S}^E, \tag{12}$$

where $\mathbf{D}_B = \mathrm{diag}(e^{jE_0^B}, e^{jE_1^B}, \cdots, e^{jE_{N-1}^B})$ is a phase inverse rotation matrix. For $i \in 0, 1, \cdots, N-1$. When E_i^A and E_i^B are in different quantization intervals, and their phase error is not sufficient to change the symbol quadrant, our scheme can still be decrypted correctly. In contrast, if a traditional quantization scheme is used, inconsistent keys will be generated and lead to decryption errors.

The above methods effectively address the problems of weak constellation dynamics and high decryption error rates, respectively. In the next section we analyze the security of the proposed scheme under some specific attacks.

III. Security Analysis

In this section, we carry out the security analysis of the proposed scheme under two attacks against a single frame and adjacent frames. Note that the eavesdropper is assumed to be fully aware of all the steps but not the secret key, and it tries to recover the information by directly applying FFT to the encrypted OFDM symbols.

A. Attack Against a Single Frame.

For pilot frames, a private pilot with random phases is employed to generate similar initial constellation patterns. The eavesdropper can only obtain the observation result of $\varphi_i^A + \theta_i$ and $\varphi_i^B + \theta_i$, but is not able to deduce $\varphi_i^A + \theta_i + \varphi_i^B$ and thus fails to obtain the information regarding the initial phase.

For data frames, an attacker may try to recover the data content or launch the traffic analysis attack to obtain information, such as communication patterns and modulation methods. By our scheme, constellation patterns are updated dynamically and are accessible only to the legitimate ends. Hence, the attacker cannot identify the constellation and carry out proper decryption. Even if the attacker can obtain part of the transmitted data and generate a closer initial value x_0, the constellations decrypted by the attacker are randomly distributed due to the introduction of chaotic sequences. The key sensitivity test results presented in Fig. 4 also demonstrated that the two encrypted OFDM symbols are significantly different after encrypting the same OFDM symbols with different keys, which will be detailed later in the next section.

B. Attack Against Adjacent Frames.

A differential attacker may exploit the relation between the results of two encrypted symbols to retrieve the relation between the initial symbols. When the traditional XOR scheme is applied in a slowly varying environment, an eavesdropper can launch a differential attack by performing the XOR operation on the ciphertext with highly consistent keys generated from adjacent frames:

$$\begin{aligned} &\mathbf{S}^E(k) \oplus \mathbf{S}^E(k+1) \\ =&\left(\mathbf{E}^A(k) \oplus \mathbf{S}(k)\right) \oplus \left(\mathbf{E}^A(k) \oplus \mathbf{S}(k+1)\right) \\ =&\mathbf{S}(k) \oplus \mathbf{S}(k+1). \end{aligned} \tag{13}$$

In contrast, the two adjacent encrypted OFDM symbols in our proposed DCR scheme are given by

$$\mathbf{S}^E(k) = E\left(\boldsymbol{C}^A(k) + \boldsymbol{\Phi}^A, \mathbf{S}(k)\right), \tag{14}$$

and

$$\mathbf{S}^E(k+1) = E\left(\boldsymbol{C}^A(k+1) + \boldsymbol{\Phi}^A, \mathbf{S}(k+1)\right), \tag{15}$$

where $\mathbf{C}^A(k)$ and $\mathbf{C}^A(k+1)$ are generated from the transmitted data of different frames by an one-way function, and $\boldsymbol{\Phi}^A$ is the channel detection result when $k = 0$. It is rather difficult by nature for an attacker to determine the the alteration rate of constellation patterns. Besides, due to the sensitivity of chaotic sequences, the differences between adjacent frames can be significant. Consequently, differential attacks become ineffective.

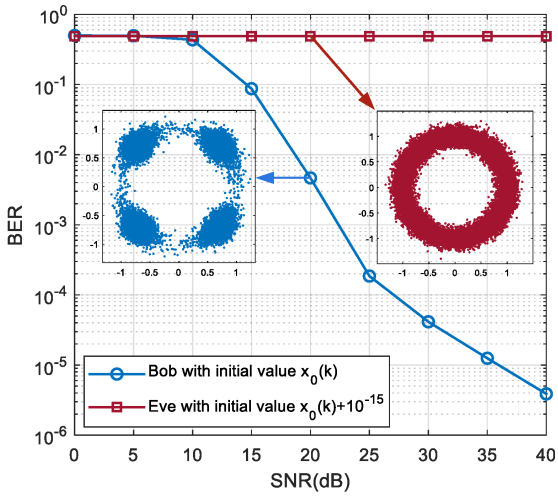


Fig. 4. BER of Bob and Eve under different initial values (QPSK).

IV. Simulation Results

In this section, simulations are conducted for OFDM systems using our proposed encryption schemes to verify the security and reliability of the proposed scheme. The simulation parameters refer to the IEEE 802.11a standard, and the number of iterations of the logistic chaotic sequence is set to be 40.

Fig. 4 exhibits the BER performance and received constellations of Bob and Eve with slightly different initial values. It can be seen that after constellation rotation encryption and noise interference, the arrangement of constellation patterns is completely disrupted and evenly distributed in the constellation space. For the legitimate receiver with $x_k^B(0)$, the OFDM symbols can be correctly decrypted after transmission, while the illegal receiver with a slight difference of 10^{-15} ends up with a BER of 0.5. It is nothing more than a random guess and thereby indicates that the illegal user is incapable of identifying the received constellation patterns and recovering any effective information. Therefore, the security advantage is verified from the key sensitivity for our proposed scheme.

In Fig. 5, the BER performance of our proposed dynamic phase encryption scheme is simulated and compared with the conventional XOR encryption scheme when $M = 10$. As the simulation results shown in this figure, we can find that as the SNR increases, the BER corresponding to different schemes gradually decreases. Compared with the XOR encryption scheme, our proposed scheme achieves better BER performance, where at a BER of 0.001, a 4.5 dB gain can be achieved when using the QPSK modulation. And as the modulation order increases, the gain in BER performance also increases. This is because that quantization will cause the loss of part of the transmitted information, leading to an increased disagreement between the encryption and decryption sequences, and ultimately resulting in the degradation of BER performance.

In Fig. 6, we investigate the robustness performance of the proposed scheme under different phase errors at SNR = 5 dB and 10 dB. The phase error ε is modeled according to (6)

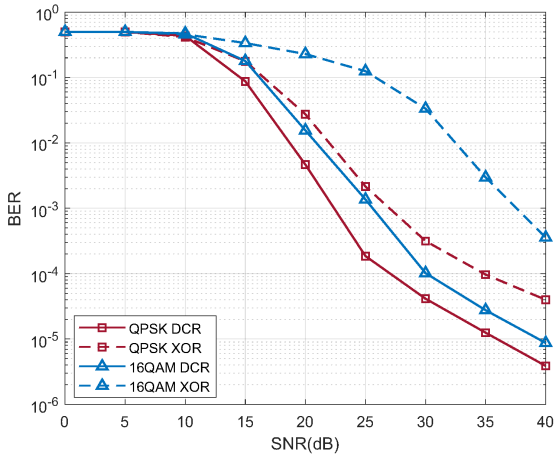


Fig. 5. BER of different encryption schemes when $M = 10$.

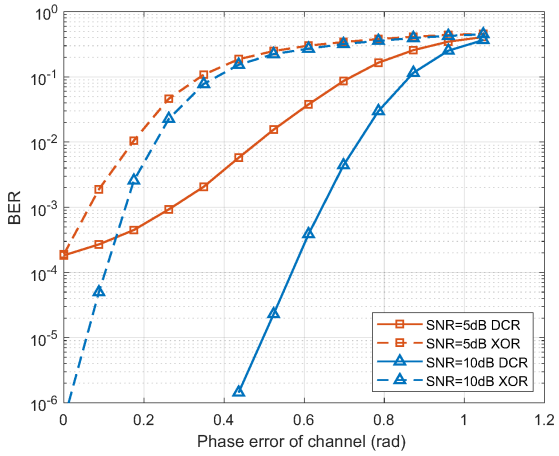


Fig. 6. BER of different encryption schemes versus phase error with different SNRs.

and Δ is increased by $\pi/36$ interval from 0 to $\pi/3$. It can be seen that the BER performance gradually decreases as the phase error increases and eventually approaches about 0.5 at around $\pi/3$. This is because the channel phase error of the system can lead to symbol misclassification, and when the channel phase estimation error is greater than $\pi/3$, the symbol is completely misclassified. In addition, as SNR increases, the phase robustness improves significantly, tolerating a larger phase error while maintaining the same BER performance.

Furthermore, when the channel phase error is less than $\pi/9$, the phase error has a less impact on the BER of the proposed analog-based DCR scheme, and the BER curve is relatively flat, while the fluctuation of the digital-based XOR scheme is larger, and the corresponding BER rises rapidly. This indicates that the DCR scheme has a certain tolerance to the channel phase estimation error and is robust in the case of channel phase error. These simulation results are consistent with the theoretical analysis, which verify the better security and reliability of the proposed DCR scheme.

V. Conclusion

In this paper, we proposed a novel PLE scheme based on dynamic constellation rotation. The scheme mainly combines the randomness of transmitted data and channels to generate adaptive constellations patterns, which support high confidentiality against malicious attacks. Moreover, we investigated the BER performance of the proposed analog-based PLE scheme and the digital-based XOR encryption scheme and their robustness against channel phase errors. Simulation results showed that our proposed scheme not only effectively prevents eavesdroppers from acquiring useful information, but also enhances the robustness against channel phase errors and improves the BER performance.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 62171121, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20211160 and in part by Jiangsu Provincial Key Laboratory of Network and Information Security under Grant BM2003201.

References

[1] F. Huo and G. Gong, "XOR encryption versus phase encryption, an in-depth analysis," *IEEE Trans. Electromagn. Compat.*, vol. 57, no. 4, pp. 903–911, Jan. 2015.

[2] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "An efficient OFDM-Based encryption scheme using a dynamic key approach," *IEEE Internet of Things J.*, vol. 6, no. 1, pp. 361–378, Feb. 2019.

[3] W. Li, D. Mclernon, J. Lei, M. Ghogho, S. A. R. Zaidi, and H. Hui, "Cryptographic primitives and design frameworks of physical layer encryption for wireless communications," *IEEE Access*, vol. 7, pp. 63 660–63 673, 2019.

[4] R. Ma, L. Dai, Z. Wang, and J. Wang, "Secure communication in TDS-OFDM system using constellation rotation and noise insertion," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1328–1332, Aug. 2010.

[5] F. Huo and G. Gong, "A new efficient physical layer OFDM encryption scheme," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2014, pp. 1024–1032.

[6] M. Xiang-ning, L. Kai-jia, and L. Hao, "A physical layer security algorithm based on constellation," in *Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT)*, 2017, pp. 50–53.

[7] G. Li, Z. Zhang, J. Zhang, and A. Hu, "Encrypting wireless communications on the fly using one-time pad and key generation," *IEEE Internet of Things J.*, vol. 8, no. 1, pp. 357–369, Jan. 2021.

[8] S. Naderi, D. B. da Costa, and H. Arslan, "Joint random subcarrier selection and channel-based artificial signal design aided PLS," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 976–980, 2020.

[9] T. Xiong, W. Lou, J. Zhang, and H. Tan, "MIO: Enhancing wireless communications security through physical layer multiple inter-symbol obfuscation," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1678–1691, 2015.

[10] A. Zuquete and J. Barros, "Physical-layer encryption with stream ciphers," in *Proc. IEEE Int. Symp. Inf. Theory*, 2008, pp. 106–110.

[11] Z. Xu, T. Yuan, Y. Gong, W. Lu, and J. Hua, "Achieving secure communication through random phase rotation technique," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2017, pp. 2073–2078.

[12] J. Liu, A. Ren, R. Sun, X. Du, and M. Guizani, "A novel chaos-based physical layer security transmission scheme for Internet of Things," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[13] G. Li, H. Yang, J. Zhang, H. Liu, and A. Hu, "Fast and secure key generation with channel obfuscation in slowly varying environments," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May. 2022, pp. 1–10.