IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 19, 2019, accepted May 22, 2019, date of publication May 28, 2019, date of current version June 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2919598

A Joint Physical Layer Encryption and PAPR Reduction Scheme Based on Polar Codes and Chaotic Sequences in OFDM System

XINJIN LU, YUXIN SHI, WEI LI, JING LEI, AND ZHIPENG PAN
Department of Communication Engineering, College of Electronic Science and Technology, National University of Defense Technology, Changsha, China

Corresponding author: Wei Li (liwei.nudt.cn@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61502518, Grant 61702536, and Grant 61601480, in part by the Natural Science Foundation of Hunan Province China under Grant 2017JJ2303 and Grant 2018JJ3609, and in part by the China Scholarship Council (CSC) Government-Sponsored Visiting Scholar Research Program.

ABSTRACT Channel coding and security are important in a communication system. The 5th generation (5G) mobile communication networks call for higher requirements of new coding technologies and encryption technologies. As an efficient coding method, polar codes have attracted more attention in recent years. Besides, the peak-to-average-power ratio (PAPR) is a major problem of the orthogonal frequency-division multiplexing (OFDM) system, which will significantly affect the performance of the OFDM system. In this paper, joint physical-layer encryption and PAPR reduction scheme is proposed, aiming to solve the PAPR problem and achieve high security of the transmission system. In this scheme, we utilize the key generation technology of wireless channels to get the initial value of chaotic sequences. Then, the chaotic sequences can be used to encrypt the information and reduce PAPR simultaneously. Moreover, we use the best information bits of polar codes to store the serial number index of chaotic sequences. The theoretic analysis and simulation results show that the proposed scheme can not only achieve high security in the physical layer but also reduce PAPR in the OFDM system without increasing system complexity and latency.

INDEX TERMS Polar codes, OFDM, PAPR, information bits, chaotic sequences.

I. INTRODUCTION

With the rapid development of wireless communication technology, 5G has become a research hotspot in the field of wireless communication. 5G will meet diverse business needs of work, life and entertainment. In addition, 5G will penetrate into all fields of industry to effectively meet the diversified business needs and realize the interconnection of all things such as industries, medical cares and transportations. The key technologies of 5G mobile communication are mainly embodied in ultra-efficient wireless transmission technology and high-density wireless network technology [1]. Channel coding technology with high performance and efficiency is also an important research direction of 5G. In 1948, Shannon proposed the mathematical theory of communication [2]. In 1962, Gallager proposed low-density parity-check (LDPC) codes [3]. In 1992, C. Berrou et al. of France proposed the revolutionary Turbo codes [4]. However, neither the Turbo code nor the LDPC had been theoretically proved to be able to reach the Shannon channel capacity. Professor Arikan first proposed the concept of polar codes, which rigorously proved that polar codes can reach the channel capacity in binary discrete memoryless channels (B.DMCs) [5]. In 2016, polar codes scheme became the final solution for enhanced mobile broadband (eMBB) scene of the 5G control channel, and successfully entered the 5G basic communication framework protocol [6]. In 2018, the 5G system that meets the 3GPP standard and supports polar codes was officially released.

Wireless communication has the characteristics of broadcasting, mobility and openness compared with the wired communication system. These characteristics make wireless communications more likely to be intercepted and eavesdropped, and thus wireless communication security issues are becoming increasingly prominent [7]. However, it should be assumed that the transmission of the physical layer is error-free in traditional secure communication technologies. The encryption algorithms at a higher layer have high computational complexity. The traditional secure communication

The associate editor coordinating the review of this manuscript and approving it for publication was Rui Wang.

technologies have not designed a security mechanism based on the channel characteristics of physical layer. Wireless physical layer security (PLS) [8] makes full use of the characteristics of channels in the wireless physical layer and both legitimate communication parties can recover the original information, while eavesdroppers (Eve) can not obtain secret information. Generally, PLS mainly includes security coding [9]–[11], cooperative interference [12], [13] and key generation [14]–[16]. Polar codes have excellent performance and special constructions due to their nested codeword structure [17] which can realize random binning [18] in PLS coding. Therefore, many scholars have applied polar codes to the model of wiretapping channel [19], [19]–[21], which promotes further development of PLS coding theory. Moreover, chaotic encryption is one of the important way to implement PLS. As an one-dimensional chaotic mapping, Logistic mapping derives from the evolution of the insect population model [22], which can produce pseudo-random sequences to encrypt data. However, most of the existing literatures do not fully consider the application of chaotic encryption in channel coding or modulation.

OFDM is a multi-carrier transmission technique widely applied in wireless communication due to its superior performance. However, PAPR is a major problem of OFDM system [23]. Occurrence of high PAPR means that linear power amplifier will work at the nonlinear amplification region, which will affect the performance of OFDM system. To reduce the PAPR of OFDM, some techniques e.g. SLM [24], [25], partial transmit sequence(PTS) [26], [27], clipping [28], [29] and coding [30], [31] are suggested. Among them, SLM technique uses the random phase sequences to produce several alternative sequences and then the sequence with minimum PAPR is transmitted, which is effective for reduction of PAPR. However, the extra random phase sequence generator or memorizer is required.

In order to solve the above problems, we consider a joint scheme based on channel coding, encryption and PAPR reduction. The main contributions of this paper are as follows:

- We use the characteristics of the wireless channels between the legitimate communication parties to design the keys as the initial values of chaos sequences. The chaotic sequences are used to encode and encrypt information bits so that the legitimate user can decrypt and decode the information correctly while the Eve cannot get the effective information.
- We adopt the idea of SLM technique in this scheme. But the PAPR reduction technique is employed on coding process, which differs from the SLM technique. The signal with the lowest PAPR in OFDM system is selected for transmission, which ensures the security and reduces the PAPR of the system at the same time.
- The chaotic sequences used in encryption are adopted as the random phase sequences generator to reduce the PAPR of OFDM systems, which do not use additional random sequences compared to SLM and simplifies the whole transmission systems.
- Taking advantages of the characteristics of channel polarization, we choose the best information bits of polar codes to convey the index bits of the chaotic sequences. With such arrangement, the better BER performance can be achieved in the proposed scheme. What's more, due to the low complexity and delay in the encoding process of polar codes, the proposed scheme will not affect the system calculation complexity and latency.

Note that this paper is a further research of our previous paper [32] published in IEEE Access, which reported a chaotic encryption algorithm based on wireless channel characteristics. The differences from the previous paper are summarized as follows. Firstly, we focus on chaotic sequences used in information bits rather than frozen bits to realize encryption. Second, we adopt the idea of SLM and give the frame of our scheme design, which could be used to reduce the PAPR and improve the safety in OFDM system.

The rest of this paper is structured as follows. In Section II, we briefly introduce the preliminaries about our scheme. The system model and the proposed scheme are provided in Section III. Section IV presents the delayed feedback chaotic encryption algorithm based on wireless channel characteristics. The simulation results and security analysis are discussed in Section V. Section VI concludes this paper.

II. PRELIMINARIES

In order to make readers better understand this scheme, the property of channel polarization is analyzed. In addition, the key generation technology and chaotic sequence generation used for encryption are described. Finally, we introduce the general scheme which adopts the idea of SLM to reduce PAPR.

A. THE SELECTION OF POLAR CODES INFORMATION BITS

As a kind of linear channel coding method, polar codes are based on channel polarization. The channel polarization includes the two processes: channels combination and channels splitting. As the number of recombined channels approaches infinity, the polarization phenomenon will appear. The channel capacity of part channels approaches 1 (the good channels) and the channel capacity of the rest part approaches 0 (the bad channels). The information bits are placed on the ''good channels'' at the transmitter. When the code length N trends to infinitude, i.e., $N \to \infty$, the shannon limit will be reached.

The symmetric channel capacities corresponding of the ''bit channels'' are shown in Fig. 1, where code length is $N = 8$ and the erasure probability is $\varepsilon = 0.5$. It can be seen that the polarization trend of ''bit channels'' is obvious.

The Fig. 2 is the channel polarization situation when the code length is $N = 1024$. We could know that most ''bit channel'' capacities are 0 or 1 and only a small part of channel capacities are between 0 and 1. Polar codes use the ''bit channels'' with high capacity to transmit the source information.

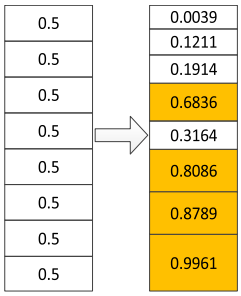


FIGURE 1. Bit channel capacities distribution when N = 8.

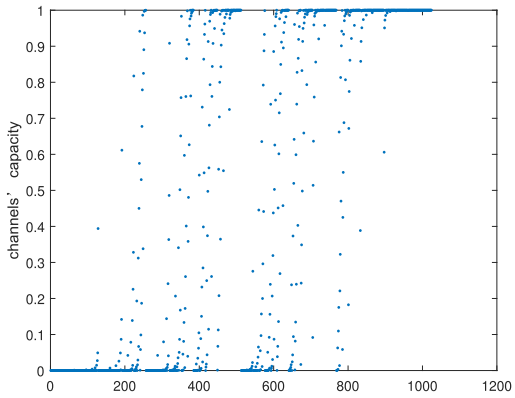


FIGURE 2. The phenomenon of channel polarization when N = 1024.

B. KEY GENERATION BASED ON WIRELESS CHANNEL CHARACTERISTICS

Due to the short-time reciprocity, time-variability and space-time uniqueness of the wireless channel, it is possible to generate the key as a natural random source. The basic idea of key generation based on characteristics of the wireless channel is that both parties of legitimate communication detect and quantify the wireless channels and then obtain the same key through information negotiation, security enhancement and other techniques in a coherent time. The key generation process is shown in Fig. 3, which can be described as follows:

1) CHANNELSC DETECTION

In coherent time, both parties of the legitimate communication transmit the detection signal periodically, and obtain the observed values of the wireless channel characteristics. The main characteristics of wireless channel used to extract keys are multipath relative delay [33] and channel state information (CSI). CSI includes channel frequency response [34] and channel impulse response (including phases and amplitude).

2) CHANNEL CHARACTERISTICS QUANTIFICATION

Both legitimate communication parties adopt the same quantification scheme and quantify the observed values of the channel characteristics to the initial keys. There are many quantification schemes, including multi-bit quantification scheme [35], double-threshold quantification scheme [36] and quantification scheme based on interactive quantification error [37].

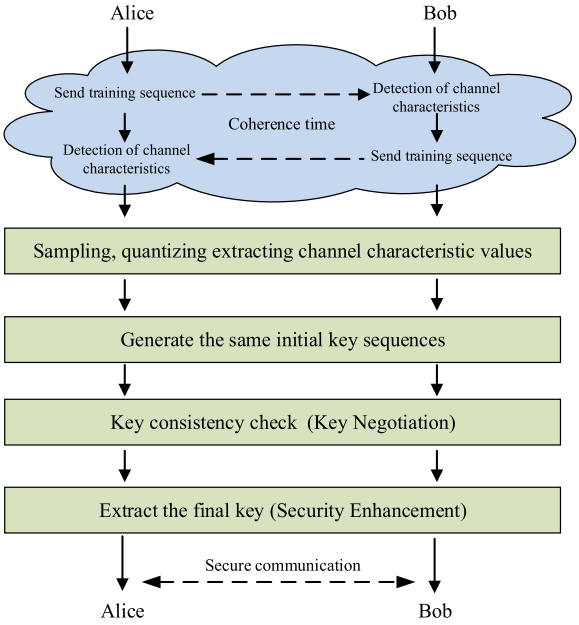


FIGURE 3. Key generation flow chart.

3) INFORMEATION NEGOTIATION

Due to influences such as the interference of channel noise, detection error and other factors, there may exist inconsistent information bits in the initial keys. Therefore, both parties of the legitimate communication achieve information interaction through a common channel to obtain consistent keys; the interaction information can be parity check or serial number of the key, etc. Ref. [38] offers practical design guidelines on secure key generation systems. The work in [39] investigated and quantified channel measurements cross-correlation relationship affected by noise and non-simultaneous measurements. So the both parties of the legitimate communication can eliminate the influence of imperfect CSI through information negotiation. The existing information negotiation methods include Cascade method [40], binary search method [41] and some error correcting code methods [42]–[44].

4) SECURITY ENHANCEMENT

In the process of channel detection and information negotiation, the illegitimate receiver may eavesdrop on some information about the key, which may bring potential threat to the security of keys. Therefore, the legitimate communication parties can use some means to eliminate some information about the keys obtained by the eavesdropper so that the keys are completely confidential. Presently, hash functions [45], [46] and extractor [46] are the main methods of security enhancement.

C. THE GENERATION OF CHAOTIC SEQUENCES

The chaotic system is considered as a pseudo random source generator because of its characteristics such as initial value sensitivity and irreversibility. Discrete chaotic sequences are generated from the discrete chaotic mapping systems and

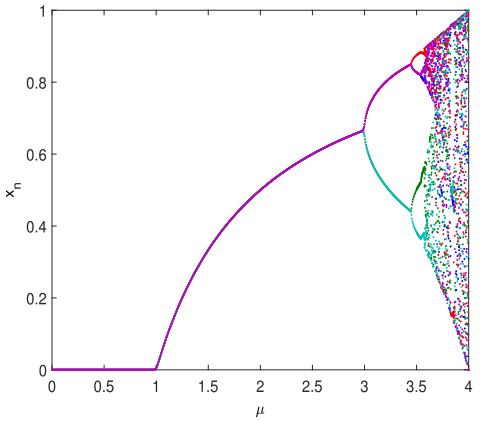


FIGURE 4. Bifurcation diagram of logistic map.

then quantified to digital chaotic binary sequences by appropriate quantification methods. The typical discrete chaotic system is a Logistic mapping, which used in this scheme. The mapping equation can be derived as

$$x_{n+1} = \mu x_n (1 - x_n) \tag{1}$$

where $x_n \in (0, 1), n = 1, 2, 3 \cdots$ and $\mu \in (0, 4]$ is systematic parameter. If the initial value x_1 and parameter μ are set, a determined chaotic sequence $\{x_n\}_{n=1}^{\infty}$ can be gained according to (1) .

The bifurcation diagram of Logistic mapping with the variation of parameters is shown in Fig. 4, which vividly depicts the transition of Logistic mapping from period doubling bifurcation to chaos. It can be seen from the diagram that the Logistic mapping shows different characteristics for different μ values. With the change of parameter μ, the system continues to undergo a period doubling bifurcation, and finally achieves the chaos. when $\mu = 4$, Logistic map distributes to the whole range of (0,1). Hence, we choose $\mu = 4$ as the parameter of Logistic mapping.

We use the frequency domain of the wireless channels to extract the phase information as the initial value of the chaotic sequences. To ensure the reciprocity of the channels in the wireless communication system, it is assumed that each channel detection between the legitimate communication parties is within the channel coherence time. In addition, all signals used in this algorithm are frequency domain signals.

D. THE PAPR OF OFDM SYSTEMS AND SLM TECHNIQUE

In comparison with a single carrier system, the outputs of the multi-carrier modulation system are the superposition of many subcarriers. If the phases of these subcarriers are coincident, the superposed subcarriers' instantaneous power would be much larger than the average power, causing the larger PAPR. The power amplifier shall be operated within wide large dynamic linearity range. Otherwise, it will cause the signal distortion when the signal peak beyond the linearity range of power amplifier. It will also lead to the intermodulation among subcarriers and out-of-band radiation so as to generate mutual interference. One of the solutions is to

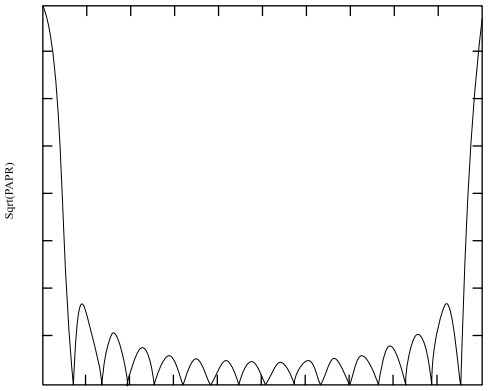


FIGURE 5. The problem of PAPR in OFDM system.

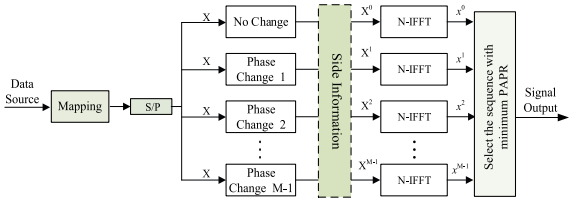


FIGURE 6. SLM structure diagram.

endow the power amplifier with quite large linearity working range. However, in turn, the large linearity working range will reduce the amplifier operation efficiency and add the complexity of transmitter facilities.

1) THE PAPR OF OFDM SYSTEMS

Comparing with the single carrier system, OFDM symbol is superposed by lots of independent modulated subcarriers which might produce the larger peak power and bring the larger PAPR. The definition of PAPR is

$$\text{PAPR}(dB) = 10\log_{10}\frac{\max\{|x_n|^2\}}{E\{|x_n|^2\}} \tag{2}$$

$$x_n = \frac{1}{\sqrt{N}}\sum_{k=0}^{1} X_k W_N^{nk} \tag{3}$$

where x_n is the output signal after the IFFT operation, $W_N = e^{-j2\pi/N}$.

As for N sub-channels of OFDM system, the signal peak power is the N times of the average power when the N sub-channels possess the same phases. In Fig. 5, taking $N = 16$ as example, it demonstrates that the PAPR is large in the OFDM system. In this case, all subcarriers are modulated by symbols with same initial phases. It can be seen that the peak power is 16 times of the average power. For the carrier wave without modulating, the PAPR is zero. Therefore, there is large PAPR within the OFDM system.

The complementary cumulative density functions (CCDFs) of PAPR are generated to measure the reduction performance of PAPR. The CCDFs can be derived as

$$\frac{1}{R}\sum_{k=1}^{R} m_k \tag{4}$$

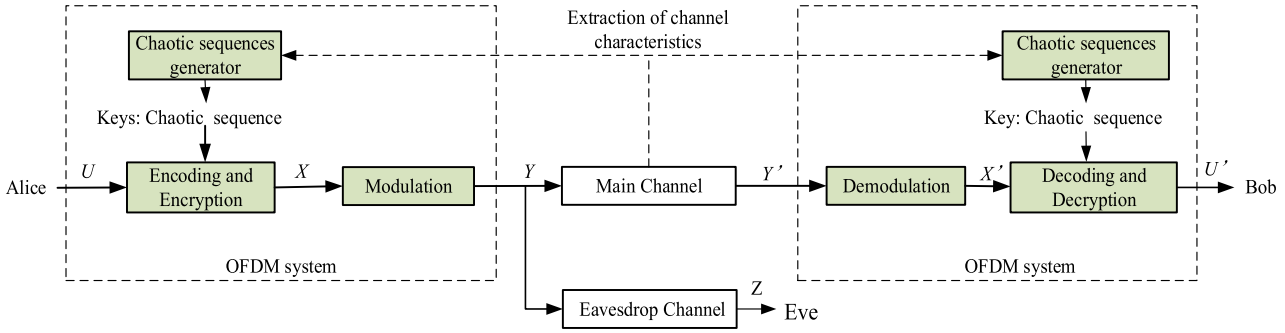


FIGURE 7. Block diagram of the communication system mode.

where

$$m_k = \begin{cases} 1, & when\ PAPR > PAPR_0 \\ 0, & other \end{cases}$$

2) THE IDEA OF SLM

The basic idea of SLM is to select and transmit the sequence with the minimum PAPR in M sequences with different phases. In Fig. 6, the system model using SLM technique is given. Through the polar encoder, the binary sequences from data source are mapped into the constellation points, given by

$$X = [X_0, X_1, \ldots, X_{N-1}] \tag{5}$$

$M-1$ different random phase sequences are produced by a random phase generator or loaded from a memorizer containing random phase sequences. The μth random phases sequence vector with can be presented by

$$P(\mu) = (P_0^{\mu}, P_1^{\mu}, \ldots, P_{N-1}^{\mu}) \tag{6}$$

where $P_i^{\mu} = \exp(j\varphi_i^{(\mu)})$ for $\mu = 1, 2, \ldots, M-1$ and $i = 0, 1, \ldots, N-1$, and $\varphi_i^{(\mu)}$ is uniformly distributed within $[0, 2\pi)$.

To achieve M sequences with different PAPR values, input data sequence multiplies the $M-1$ random phase sequences, respectively. Thus, the μth sequence after multiplication is derived as

$$\begin{aligned} X(\mu) &= (X_0^{(\mu)}, X_1^{(\mu)}, \ldots, X_{N-1}^{(\mu)}) =< X \bullet P(\mu) > \\ &= (X_0 P_0^{\mu}, X_1 P_1^{\mu}, \ldots, X_{N-1} P_{N-1}^{\mu}) \end{aligned} \tag{7}$$

where $< \bullet >$ represents the point multiplication. Then IFFT calculation will be implemented on the M different output sequences. For the μth sequence, it can be shown as

$$x_{\mu} = \mathrm{IFFT}[X(\mu)], \quad (n = 0, \ldots, N-1) \tag{8}$$

Among these M sequences, the sequence with the minimum PAPR is selected for transmission. The side information that denotes the index of random phase sequence corresponding to the minimum PAPR sequence is added into the sequence. It worth noted that the correct detection of side information is important to the recover the OFDM symbols. Hence, better channel conditions are required to convey the side information.

III. THE SYSTEM MODEL AND SCHEME DESIGN

The block diagram of the system model of this program is shown in Fig. 7. In the OFDM system, the sender (Alice) sends a message to the legitimate recipient (Bob), while the eavesdropper (Eve) wants to intercept the transmitted message. Alice and Bob extract the key through the primary channel. Due to the space-time uniqueness of the wireless channel, Eve does not know any information about the key. When Alice transmits a message to Bob, the plaintext message is encoded and encrypted by encoding and encryption module to get ciphertext X. And then X is modulated to the output waveform Y. When Bob receives Y', he first gets X' through the demodulation module, and then gets U' through the decoding and decryption module. Since the information obtained by Eve is the encrypted chaotic ciphertext Z, the difficulty of decoding increases greatly. Moreover, the reduction of the PAPR is employed with encrytion process simultaneously in OFDM system, which is further depicted next.

The block diagram of transmitter is shown in Fig. 8, which takes steps as follows:

- Step 1: According to the channel characteristics, the key is obtained from key generation which can be seen clearly in Fig.3. Then the initial value of the key with quantization is sent to the chaotic sequence generator to generate chaotic sequences. According to the length of the codes, the chaotic sequences are divided into $V = 2^v (v = 0,1,2,\ldots)$ segments, where v is bits of serial number index. E.g. as shown in Fig. 9, if $v = 2$, i.e. $V = 4$ segments, and the chaotic sequences are represented by the serial number indices 00, 01, 10 and 11. The serial number index and the information to be transmitted are placed on the information bits of the polar codes. Above all, the serial number index is placed on the best information bits of the polar codes.
- Step 2: We encrypt the bit positions of polar codes with chaotic sequences except the bits of serial number index positions, as shown in Fig. 10. The chaotic sequences are chosen by the serial number index. For example, when the code length is 128 bits and the code rate of polar codes is 0.25, 2 of information bits are used to store the serial number index while the other 30 bits are encrypted with chaotic sequences by XOR algorithm.

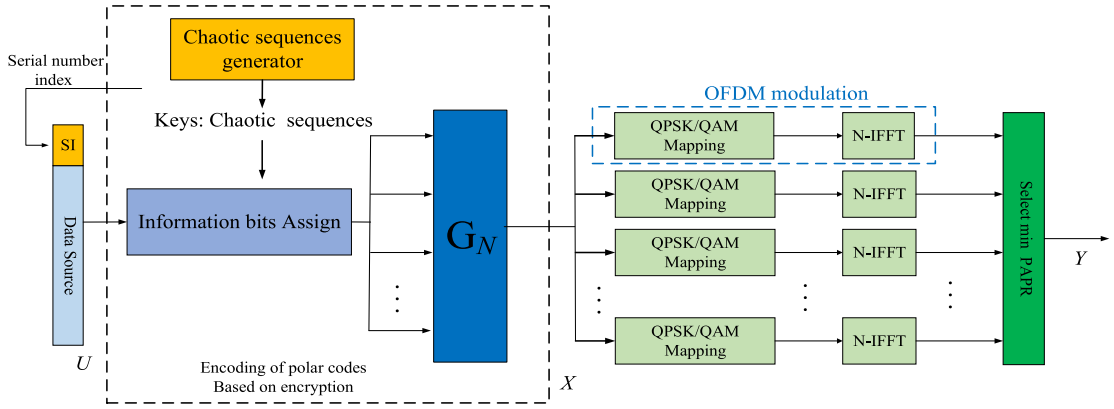


FIGURE 8. The block diagram of the sender.

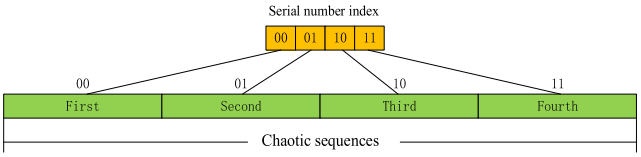


FIGURE 9. The serial number indices of chaotic sequences.

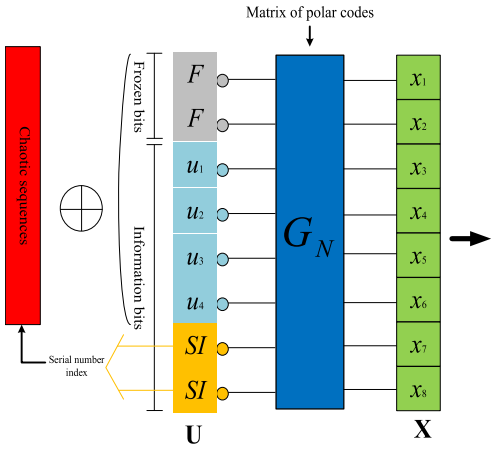


FIGURE 10. The process of encryption and encoding.

- Step 3: The sender Alice encodes the encrypted information sequences U with polar codes, which can be presented by

$$X = UG_N(A) + U_{A^c}G_N(A^c) \tag{9}$$

where N ($N = 2^n$) is the code length, and $G_N(A)$ is the sub-matrix of G_N. The matrix is composed of row vectors corresponding to the elements in the set, and the encoding is completed in the binary finite field.
- Step 4: The coded signal is fed into the OFDM system, and the PAPR of different chaotic sequences is obtained. The signal with minimum PAPR is selected for transmission.

From the steps above, it can be observed that the encryption process is combined with the PAPR reduction, which removes the random phase sequence generator compared to SLM technique. Moreover, due to the different performances of polar channels, we select the channel with highest channel capacity to convey serial number index, which can enhance the performance of the system. Compared to the general system split the two process, it worth noted that polar encoding in the proposed scheme are required to employed on V versions of sequence. However, the encoding process of polar codes is provided by a very simple G_N matrix, which means that the V encoding do not affect the complexity of the system obviously.

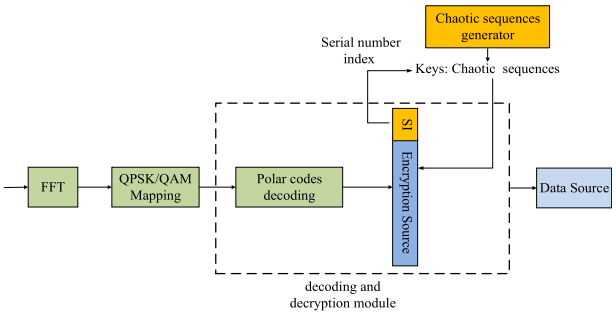


FIGURE 11. The block diagram of the receiver.

In the receiver, the block diagram of receiver is depicted in Fig. 11, which can be conducted as follows:

- Step 1: Demodulate the received signal. Note that the signal we receive is the one with the minimum peak-to-mean ratio, so we only need to demodulate according to the corresponding modulation mode.
- Step 2: Use SC decoder [47] to decode, and the decoding decision expression is

$$\hat{u}_i = \begin{cases} u_i, & i \in A^c \\ h_i(y_1^N, \hat{u}_1^{i-1}), & i \in A \end{cases} \tag{10}$$

where A is the set of information bits and A^c is the set of frozen bits. $h_i(y_1^N, \hat{u}_1^{i-1})$ can be described as

$$h_i(y_1^N, \hat{u}_1^{i-1}) \triangleq \begin{cases} 0, & L_N^i(y_1^N, \hat{u}_1^{i-1}) \geq 1 \\ 1, & otherwise \end{cases} \tag{11}$$

SC decoder is used to calculate the transfer probability of each bit channel, and then the Likelihood-Ratio (LR) information of each bit channel is iteratively computed to make a hard decision for each transmitted information. The Likelihood-Ratio information is defined as

$$L_N^i(y_1^N, \hat{u}_1^{i-1}) = \log \frac{W_N^i(y_1^N, \hat{u}_1^{i-1}|0)}{W_N^i(y_1^N, \hat{u}_1^{i-1}|1)} \quad (12)$$

- Step 3: Receiver could get the same initial key because of key generation. The initial key is sent to the same chaotic sequence generator to generate the same chaotic sequences. After decoding, receiver could find the serial number index which is placed on the best information bits of the polar codes and then search out the corresponding chaotic sequence segment by use of the serial number index. E.g. as shown in Fig. 9, if receiver gets 00 from the best information bits, he would the first chaotic sequences which are corresponding to the serial number indices 00. Finally, the received sequences could be decrypted with chaotic sequences by XOR algorithm and then the decrypted information sequence can be obtained.

For the receiver, the processes of demodulation, decoding can be employed as usual. Firstly, the receiver can directly get the side information from the best information bits after polar decoding because the best information bits are not encrypted by transmitter. Then the segments of chaotic sequences used by transmitter can be determined by the side information. Finally, the receiver use the segments of chaotic sequences to decrypt the information bits. Accordingly, there is no extra complexity for the receiving end.

IV. SIMULATION RESULTS

In this section, we focus on the PAPR reduction performance of the proposed scheme compared to SLM technique and BER performance under various channels.

In Fig. 12, the PAPR reduction improvement of the proposed Polar-SLM scheme is compared with the traditional SLM scheme at different code length N. The number of chaotic sequence $V = 4$. It can be observed that the proposed scheme can achieve the same PAPR reduction performance as the SLM scheme with $N = 128$, 256 and 512. Therefore, the proposed Polar-SLM scheme is proved to effectively reduce the PAPR in OFDM as the traditional SLM at different code length.

In Fig. 13, The proposed Polar-SLM scheme is employed with BPSK, QPSK and 16QAM while the number of chaotic sequences segments $V = 8$ and code length $N = 128$. It can be seen that the Polar-SLM achieves the prominent reduction of PAPR under different modes of modulation.

The relationship of PAPR reduction performance and the number of chaotic sequence V is given in Fig. 14, where BPSK is employed and the code length $N = 128$. It can be seen that the performance of the PAPR reduction is improved gradually with the increase of V, since more chaotic

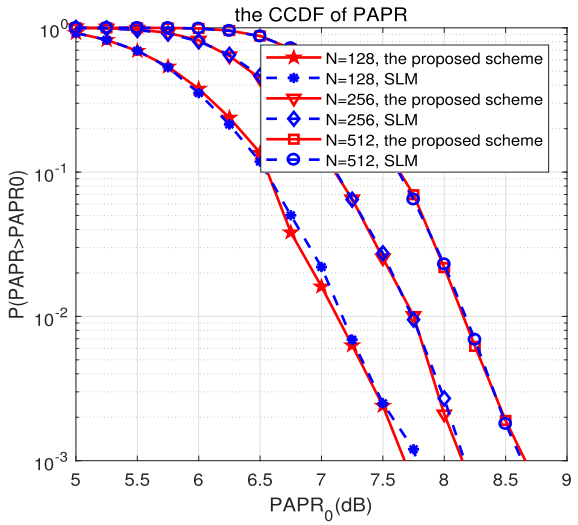


FIGURE 12. The PAPR comparison of SLM and polar-SLM methods with different code lengths.

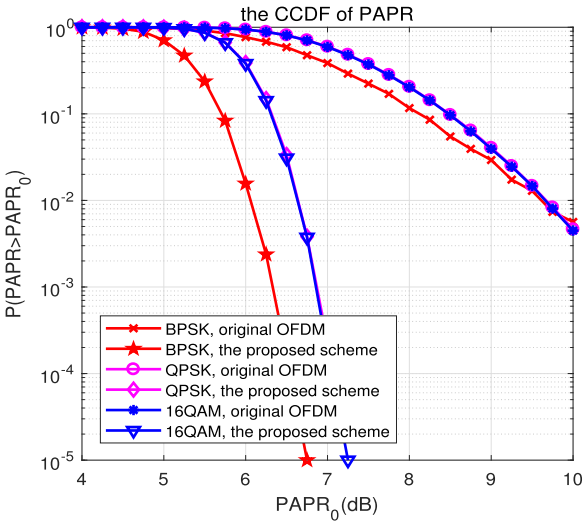


FIGURE 13. The influence of different modulation methods on proposed scheme and original scheme.

sequences segments with different PAPR values can be chosen. Therefore, transmitter is capable of choosing the serial number index of chaotic sequences to adjust PAPR reduction performance according to the characteristics of the power amplifiers.

As shown in Fig. 15 and Fig. 16, comparison of BER performance between the proposed scheme and the OFDM system using polar codes and SLM technique is presented. We adopt BPSK and QPSK modulation format over AWGN channel. Note that encoding and PAPR reduction processes are combined in the proposed scheme where best channels of polar codes are selected for side information, while in normal OFDM scheme, polar encoding process and SLM process are divided. The code lengths are $N = 64$ and $N = 128$ respectively, and the number of serial number indices is $v = 4$.

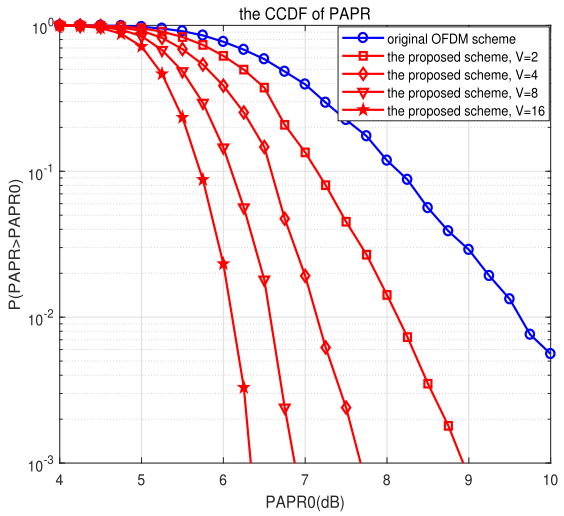


FIGURE 14. PAPR of proposed scheme with different indices lengths.

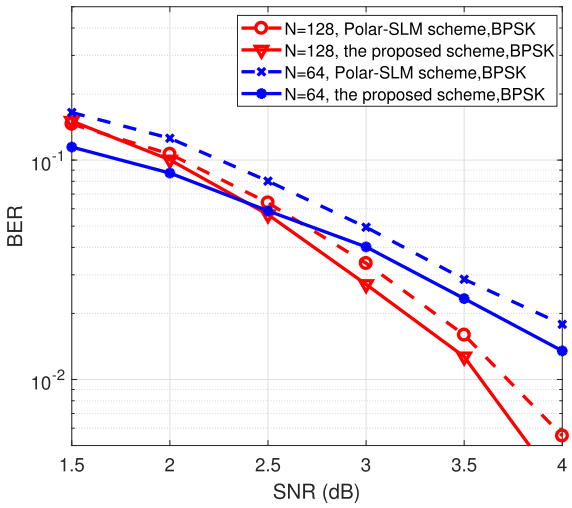


FIGURE 15. BER performances comparisons of the proposed scheme and polar coding-SLM at code lengths $N = 64$ and $N = 128$, BPSK over AWGN channel.

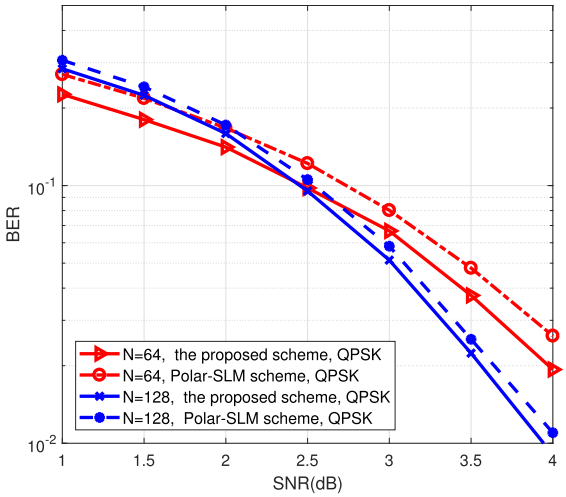


FIGURE 16. BER performances comparisons of the proposed scheme and polar coding-SLM at code lengths $N = 64$ and $N = 128$, QPSK over AWGN channel.

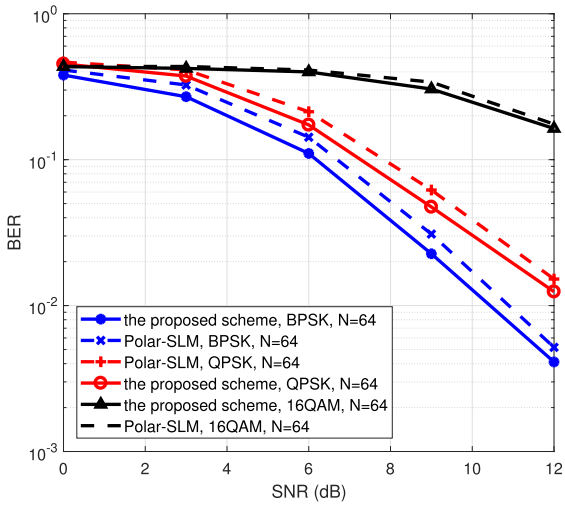


FIGURE 17. BER performances comparisons of the proposed scheme and polar coding-SLM at code lengths $N = 64$, BPSK, QPSK and 16QAM over Rayleigh fading channel.

It can be seen that the proposed scheme achieves better BER performances in different code lengths with different modulation formats.

In order to further verify the feasibility of the scheme, we carry out BER simulation under frequency selective Rayleigh fading channel, the taps of which are 10. It is important to note that the BER simulation is obtained under ideal channel case. As shown in Fig. 17 and Fig. 16, BER performances comparisons of the proposed scheme and polar coding-SLM with different modulation formats over Rayleigh channel are presented. We adopt BPSK, QPSK and 16QAM modulation format over Rayleigh channel, and the code lengths are $N = 64$ and $N = 128$ respectively. Similarly, polar encoding and PAPR reduction processes are combined in the proposed scheme and the number of serial number indices is $v = 4$. It can be seen that the proposed scheme achieves better BER performances over Rayleigh channel with different modulation formats.

We can see that compared with polar-SLM scheme the proposed scheme can get better performance over AWGN channel or Rayleigh channel. It can be explained that the combined channels with large channel capacity are more reliable for transmission of side information.

The strong key sensitivity of a good security encryption strategy is required in this scheme, which indicates that the eavesdropper cannot obtain the source data when there is a very small difference between the keys. In order to test the sensitivity of initial key values, we employ the C++ high-level programming language and the GNU multiple precision arithmetic library (GMP). The test results are shown in table 1. It can be seen that when the initial value is selected between (0, 1) randomly, the difference is 10^{-10}, and the

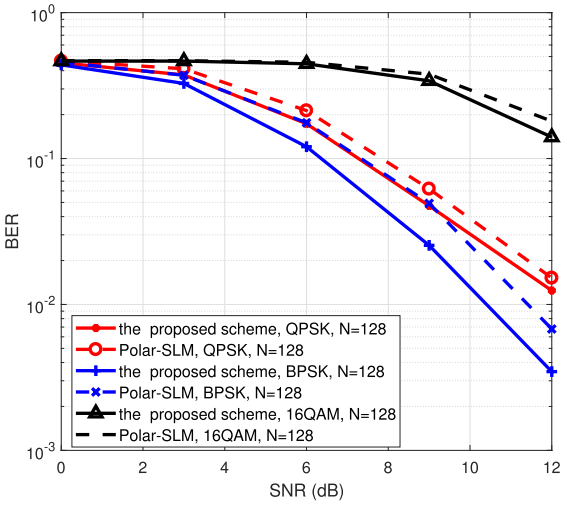


FIGURE 18. BER performances comparisons of the proposed scheme and polar coding-SLM at code lengths $N = 128$, BPSK, QPSK and 16QAM over Rayleigh fading channel.

TABLE 1. Sensitivity detection results of chaotic sequence key.

Key difference accuracy	Chaos sequence differences
10^{-10}	50.38%
10^{-20}	50.17%
10^{-30}	50.03%
10^{-40}	49.97%
10^{-50}	49.87%

difference rate of chaotic sequences is around 50%. There are half difference in chaotic sequences. Eve cannot decipher the received ciphertext information, i.e., the algorithm has high key precision and strong key sensitivity.

V. CONCLUSION

In this paper, the reduction of PAPR in OFDM system is combined well with the encryption using the coding characteristic of polar codes. Based on the characteristics of wireless channels, chaotic sequences are provided for encryption. Inspired by the idea of SLM, chaotic sequences are utilized for PAPR reduction and the system model is simplified. Moreover, side information containing the bits of serial number indices is conveyed by the largest channel capacity of polar code, leading to the improvement of BER performance. Therefore, the proposed scheme can both effectively reduce the PAPR of the OFDM system and realize encryption in the coding process, which enhances the security and reliability of the system.

ACKNOWLEDGMENT

This paper was presented in part at the 2018 IEEE Access, Xinjin Lu, Jing Lei, Wei Li, Ke Lai, Zhipeng Pan, "Physical Layer Encryption Algorithm Based on Polar Codes and Chaotic Sequences", December, 2018.

REFERENCES

[1] C. J. Zhang, J. Ma, G. Y. Li, Y. Kishiyama, S. Parkvall, G. Liu, and Y. H. Kim, "Key technology for 5G new radio," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 10–11, Mar. 2018.
[2] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.
[3] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, Jan. 1962.
[4] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2002, pp. 1064–1070.
[5] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2008.
[6] *NR and NG-RAN Overall Description—Rel. 15*, document TS 38.212, 3GPP, 2018.
[7] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.
[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[9] R. Hooshmand and M. R. Aref, "Polar code-based secure channel coding scheme with small key size," *IET Commun.*, vol. 11, no. 15, pp. 2357–2361, 2017.
[10] C. Li, G. Xuan, C. W. Tan, and R. W. Yeung, "Fundamental limits on a class of secure asymmetric multilevel diversity coding systems," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 737–747, Apr. 2018.
[11] Y. Huang, W. Li, and J. Lei, "Concatenated physical layer encryption scheme based on rateless codes," *IET Commun.*, vol. 12, no. 12, pp. 1491–1497, 2018.
[12] K. Pham and K. Lee, "Non-cooperative interference alignment for multicell multiuser MIMO uplink channels," *IET Commun.*, vol. 11, no. 5, pp. 648–654, 2017.
[13] H. Zeng, X. Qin, Y. Xu, S. Yi, Y. T. Hou, and W. Lou, "Cooperative interference neutralization in multi-hop wireless networks," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 889–903, 2018.
[14] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, Aug. 2017.
[15] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.
[16] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.
[17] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Lett.*, vol. 14, no. 8, pp. 752–754, Aug. 2010.
[18] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. 2011.
[19] W. Hao, L. Yin, and H. Qin, "Secrecy transmission scheme based on 2-D polar coding over block fading wiretap channels," *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 882–885, May 2018.
[20] R. Hooshmand and M. R. Aref, "Efficient polar code-based physical layer encryption scheme," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 710–713, Dec. 2017.
[21] M. A. M. Sayed, R. Liu, and C. Zhang, "A novel scrambler design for enhancing secrecy transmission based on polar code," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1679–1682, Aug. 2017.
[22] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, Jun. 1976.
[23] G. Wunder, R. F. H. Fischer, H. Boche, S. Litsyn, and J.-S. No, "The PAPR problem in OFDM transmission: New directions for a long-lasting problem," *IEEE Signal. Process. Mag.*, vol. 30, no. 6, pp. 130–144, Nov. 2013.
[24] S.-H. Wang, K.-C. Lee, and C.-P. Li, "A low-complexity architecture for PAPR reduction in OFDM systems with near-optimal performance," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 169–179, Jan. 2016.
[25] D. J. G. Mestdagh, J. L. G. Monsalve, and J.-M. Brossier, "GreenOFDM: A new selected mapping method for OFDM PAPR reduction," *Electron. Lett.*, vol. 54, no. 7, pp. 449–450, 2018.

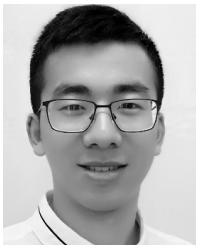
[26] M. Singh and S. K. Patra, "Partial transmit sequence optimization using improved harmony search algorithm for PAPR reduction in OFDM," *ETRI J.*, vol. 39, no. 6, pp. 782–793, 2017.
[27] M. Yoshida, H. Nashimoto, and T. Miyajima, "PTS-based PAPR reduction by iterative *p*-norm minimization without side information in OFDM systems," *IEICE Trans. Commun.*, vol. E101, no. 3, pp. 856–864, 2018.
[28] J. Hou, X. Zhao, F. Gong, H. Fei, and J. Ge, "PAPR and PICR reduction of OFDM signals with clipping noise-based tone injection scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 222–232, Jan. 2017.
[29] Y. Lin, K. Song, and M. S. Yun, "Iterative clipping noise recovery of OFDM signals based on compressed sensing," *IEEE Trans. Broadcast.*, vol. 63, no. 4, pp. 706–713, Dec. 2017.
[30] M. R. Motazedi and R. Dianat, "Reduction of PAPR in coded OFDM using fast Reed–Solomon codes over prime Galois fields," *Int. J. Electron.*, vol. 104, no. 2, pp. 328–342, 2016.
[31] C.-Y. Hsu and H.-C. Liao, "Generalised precoding method for PAPR reduction with low complexity in OFDM systems," *IET Commun.*, vol. 12, no. 7, pp. 796–808, 2018.
[32] X. Lu, J. Lei, W. Li, K. Lai, and Z. Pan, "Physical layer encryption algorithm based on polar codes and chaotic sequences," *IEEE Access*, vol. 7, pp. 4380–4390, 2019.
[33] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual OFDM Subcarrier's channel response," in *Proc. GLOBECOM Workshops*, Dec. 2016, pp. 1–6.
[34] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2009.
[35] S. T. Ali, V. Sivaraman, and D. Ostry, "Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput.*, Hong Kong, Dec. 2010, pp. 644–650.
[36] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2010.
[37] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 2065–2078, Jul. 2017.
[38] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.
[39] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *Proc. IEEE Int. Workshop Signal Process. Adv. Wireless Commun.*, Jul. 2016, pp. 1–5.
[40] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," Dept. IEEE Educ. Activities, Tech. Rep., Sep. 2013.
[41] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based PID controller," Dept. IEEE Educ. Activities, Tech. Rep., Sep. 2013.
[42] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2013, pp. 927–935.
[43] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014.
[44] D. Chen, N. Cheng, N. Zhang, K. Zhang, Z. Qin, and X. Shen, "Multi-message authentication over noisy channel with polar codes," in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst.*, Orlando, FL, USA, Oct. 2017, pp. 46–54.
[45] D. Chen, N. Zhang, R. Lu, X. Fang, K. Zhang, Z. Qin, and X. Shen, "An LDPC code based physical layer message authentication scheme with prefect security," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 748–761, Apr. 2018.
[46] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Apr. 2011, pp. 1422–1430.
[47] A. Alamdar-Yazdi and F. R. Kschischang, "A simplified successive-cancellation decoder for polar codes," *IEEE Commun. Lett.*, vol. 15, no. 12, pp. 1378–1380, Dec. 2011.

XINJIN LU received the B.Sc. degree in communication engineering from Hunan University (HNU), Changsha, China, in 2016, where she is currently pursuing the M.Sc. degree with the Department of Communication Engineering, School of Electronic Science. Her research interests include channel coding and physical-layer security.

YUXIN SHI received the B.Sc. degree in communication engineering from the National University of Defense Technology (NUDT), Changsha, Hunan, China, in 2016, where he is currently pursuing the M.Sc. degree with the Department of Communication Engineering, School of Electronic Science. His research interests include index modulation, wireless transmission, and physical-layer security.

WEI LI received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from the National University of Defense Technology (NUDT), Changsha, China, in 2002, 2006, and 2012, respectively, all in communication engineering. He is currently a Lecturer with the Department of Communication Engineering, School of Electronic Science and Engineering, NUDT. He is also a Visiting Researcher with the University of Leeds. His research interests include wireless communications, wireless network resource allocation, and physical-layer security. He received the Exemplary Reviewer Award from the IEEE COMMUNICATION LETTERS, in 2014.

JING LEI received the B.Sc., M.Sc., and Ph.D. degrees from the National University of Defense Technology (NUDT), Changsha, China, in 1990, 1994, and 2009, respectively. She was a Visiting Scholar with the School of Electronics and Computer Science, University of Southampton, U.K. She is currently a Distinguished Professor with the Department of Communications Engineering, College of Electronic Science, NUDT, and the Leader of the Communication Coding Group. She has published many papers in various journals and conference proceedings and five books. Her research interests include information theory, LDPC, space–time coding, advanced multiple access technology, physical-layer security, and wireless communication technology.



ZHIPENG PAN received the B.S. and M.S. degrees in information and communication engineering from the National University of Defense Technology (NUDT), Changsha, China, in 2014 and 2016, respectively, where he is currently pursuing the Ph.D. degree with the Department of Communication Engineering, School of Electronic Science. His research interests include advanced multiple access techniques, channel coding, and iterative decoding.