IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SPECIAL SECTION ON ADVANCES IN CHANNEL CODING FOR 5G AND BEYOND

Received November 25, 2018, accepted December 13, 2018, date of publication December 20, 2018,
date of current version January 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2888883

Physical Layer Encryption Algorithm Based on Polar Codes and Chaotic Sequences

XINJIN LU[1], JING LEI[1], WEI LI[1,2], KE LAI[1], AND ZHIPENG PAN[1]

[1]Department of Communication Engineering, College of Electronic Science and Engineering, National University of Defense Technology, Changsha, China
[2]University of Leeds, Leeds LS2 9JT, U.K.

Corresponding author: Jing Lei (leijing@nudt.edu.cn)

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 Researches on 5th generation mobile communication networks (5G) are emerging to meet the demands of rapidly developing communications applications. The reliability and security of data have become key factors of its development, and thus 5G has put forward higher requirements for new coding and encryption technologies. In this paper, a physical layer encryption algorithm based on polarization codes and chaotic sequences is proposed to improve the reliability and confidentiality of transmission. In our scheme, chaotic sequences are allocated in the frozen bits of polar codes. Therefore, error correction and encryption can be performed simultaneously. Since the frozen bits are unknown to the eavesdroppers, it is difficult for them to decode the transmitted bits without the knowledge of the chaotic sequences. To further improve the security, we propose to generate the chaotic sequences by using the channel state information. Besides, the chain effects of delayed feedback are applied to increase the decrypted complexity of the eavesdroppers in this paper. Theoretic analysis and simulation results both show that the proposed algorithms can achieve high security without any error rate performance loss.

INDEX TERMS Physical layer encryption, polar codes, chaotic sequences, frozen bits.

I. INTRODUCTION

With the development of wireless communication, the reliability and safety of data has become a key point of wireless communication. Owing to the requirements of low latency and limited physical resources in the forthcoming 5G, it is challenging to guarantee the security in the scenarios such as massive machine type of communication (mMTC), ultra-reliable & low latency communication (uRLLC) and enhanced mobile broadband (eMBB). Thus, the reliability, effectiveness and information confidentiality are the key research topics of 5G communications.

The channel coding technology can prominently improve the reliability and effectiveness of information transmission. In 1948, Claude Shannon laid the foundation of the theories of channel encoding in ''the mathematical theory of communication'' [1]. From then on, the researchers continued to promote the technologies of channel encoding to approach to the Shannon limit. In 2006, Arikan found that the reunion and separation of channels could improve the cutoff rates of discrete memoryless channels [2]. He proposed the concept of polarization and the realization of coding and decoding and proved that the progressive performance could reach the Shannon limit under the theory of binary-input discrete memoryless channels (B-DMC) [3]. After that, the polar codes are widely used for multiple channels and multilevel systems, and selected into one of the alternative technologies of 5G communication.

The construction of the generator matrix and the determination of the information set are important processes of polar code encoding. Reference [4] theoretically gave the conditions for generator matrix which can achieve the channel polarization. The information bits are the set transmitted with reliable channels, which are generally selected by Bhattacharyya parameter. For binary additional Gaussian white noise channel (B-AWGN), a method for calculating Bhattacharyya parameter was proposed in [5]. In the encoding process, the channels with small value of Bhattacharyya parameters are selected to transmit information bits, and these channels with big value of Bhattacharyya parameters are selected to transmit frozen bits. The frozen bits are usually sequences of zero known by both parties of communication. Because of this, these frozen bits cause a lot

of waste in communication, especially when the code rate is low.

The concept of physical layer security (PLS) was initially proposed by Wyner from an information theoretical perspective. In recent years, PLS researches mainly focused on the practical perspective [6]–[13]. Channel coding and encryption are considered as independent modules in conventional communication systems. Transmission reliability is achieved through error correction over the physical layer [14], while the security is achieved through cryptographic algorithm at higher layers. With the rapid development of wireless communication, the complexity and delay requirements for data processing in communication system are also increased. The joint design of error correction and encryption over physical layer is a promising technique to provide a transmission system with low complexity and delay [15]–[17]. A public-key encryption model based on algebraic coding theory was proposed in [11], in which Goppa codes are used as error correction codes. However, this scheme requires large computing cost and key size. Inspired by the idea of encryption and error correction coding, many researchers have improved the McEliece model from different aspects [15]–[19]. But these methods of encryption and error correction coding take up extra resources and lack of correlation between bits. Therefore, the effective combination of coding and encryption to improve transmission efficiency and security requires more effort.

In 1963, American meteorologists discovered the first Lorenz chaotic system in the course of studying meteorological changes. Later, the study on chaos in the nonlinear system attracted wide attention. In 1976, Rossler proposed a simple topological structure with only one nonlinear term after Lorenz chaos system [20]. In the same year, astronomer Henon proposed a two-dimensional two-parameter discrete iteration Henon chaotic map [21]. RM [22] proposed a method to generate one-dimensional Logistic discrete chaotic mapping with good stochastic characteristics. It is found that Logistic mapping could be transferred from the ordered state to the chaotic state through scale transformation, and the universality constant and scaling property in the famous bifurcation process of octave were proposed in [23]. In addition, chaos is widely used in the design of communication systems [24]–[26]. R.M atthews defined a generalized Logistic mapping, and used it to produce pseudo-random sequence to encrypt data [27]. Since then researchers began to combine chaotic systems with encryption, namely chaotic encryption. A number of chaotic encryption methods have been proposed successively. However, most of the existing literature does not consider the application of chaotic encryption in channel coding.

In this paper, we design a physical layer encryption algorithm based on frozen bits of polar codes and chaotic sequences. To further improve the security, we design a delayed feedback chaotic encryption algorithm based on polar code according to the characteristics of wireless channel, chaotic sequences and polar codes encoding structure. In summary, the contributions of the paper are as follows:

- A chaotic sequence generator is used to generate the chaotic sequences and the sequences are stored in the frozen bits. This method not only fully improves the use of the polar code, but also prevents eavesdroppers from getting effective information easily.
- We use the randomness and differences of the wireless channel between the legitimate user and the eavesdropper to design the keys. Then we use the keys as the initial values to generate the chaos sequence which used in this paper.
- The chaos sequence is used to encode and encrypt information bits so that the legitimate user can decrypt correctly and decode the information while the eavesdroppers cannot decode the effective information.
- Besides, the chain effect of lag feedback makes randomness distributed among multiple groups. And the different exchange sequences which are produced by the same information grouping makes it even harder for the cryptanalysis.

Note that this paper is an extended version of our previous conference paper [28] in which we did not focus on chaotic sequences used in frozen bits and only reported a delayed feedback chaotic encryption algorithm based on wireless channel characteristics. The differences from the conference paper are summarized as follows: First, we deeply introduce the key generation based on wireless channel characteristics and digital encryption method based on chaotic sequence in Section II. Second, we propose a physical layer encryption algorithm based on frozen bits of polar codes and chaotic sequences in Section III. Third, we also theoretically and experimentally discuss the physical layer encryption algorithm based on frozen bits of polar codes, which is to be described in Sections V-A.

The rest of this paper is structured as follows. In Section II, we briefly introduce the physical layer encryption transmission scheme. The scheme of chaotic sequences used in frozen bits is proposed in Section III. Section IV presents the delayed feedback chaotic encryption algorithm based on wireless channel characteristics. The simulation results and secrecy analysis are discussed in Section V. Section VI concludes this paper.

II. PHYSICAL LAYER ENCRYPTION TRANSMISSION TECHNOLOGY

The conventional PLS scheme achieves security transmission by introducing artificial noise, beamforming and cooperative relay in the Wyner eavesdropping model, which is based on a strong assumption that the main channel is ‘‘better’’ than the eavesdropping channel. In fact, due to the complexity of the wireless channel environment, we have inability to predict the CSI of eavesdroppers [29]. Some elementary and solid works aiming at extracting keys from channels were proposed in [30]. This paper mainly focuses on the physical layer encryption technology based on wireless channel

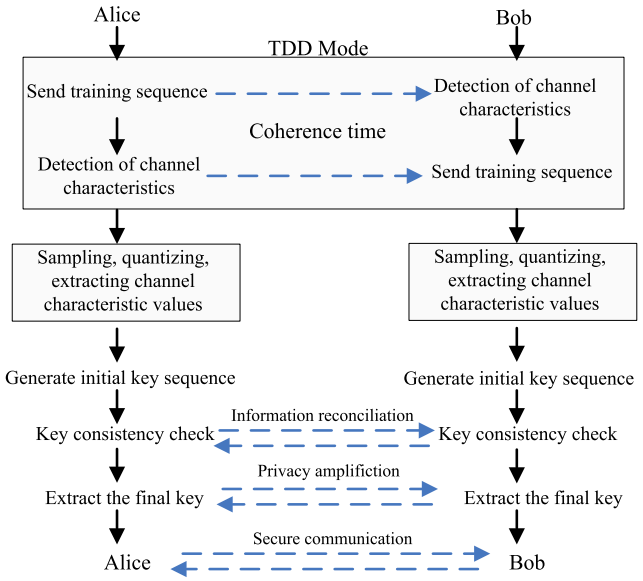


FIGURE 1. Key extraction flow chart.

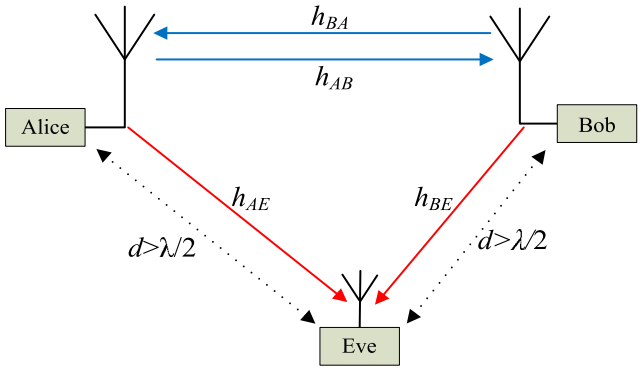


FIGURE 2. The system model.

characteristics, aiming at encrypting and protecting physical layer information such as physical layer channel coding.

A. 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 keys from channels 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 channel and then obtain the same key through information negotiation, security enhancement and other techniques in a coherent time. The extraction process is shown in Fig. 1, which includes channel probing [31], [32], quantification [33]–[35], information reconciliation [36]–[39] and privacy amplification [40], [41].

As shown in Fig. 2, Alice and Bob are legitimate communication nodes that attempt to extract phase information from channels and communicate securely. Eve is an eavesdropper who attempts to steal the channel phase information during communications between Alice and Bob. h_{AB} and h_{BA} are the

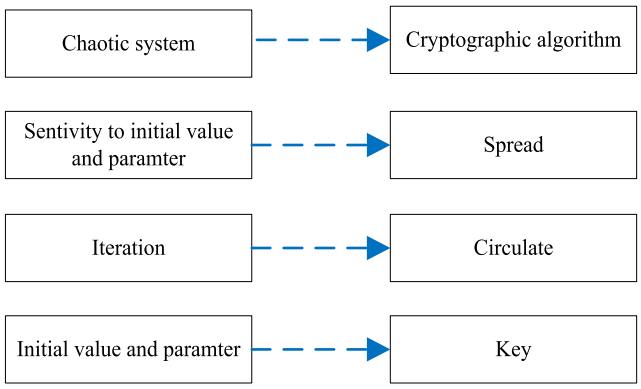


FIGURE 3. The comparison between chaotic systems and traditional encryption methods.

reciprocal channels between Alice and Bob whereas h_{AE} and h_{BE} are the channels between Alice, Bob and Eve. Assuming Eve is a passive eavesdropper, and each node adopts a half-duplex mode equipped with one antenna. At the same time, in order to ensure the reciprocity between the uplink channels h_{AB} and downlink channels h_{BA} during the channel coherence time. The legitimate communication parties communicate in time division multiplexing (TDD) mode. There are two cases:

In the first case, the distance between Eve and the legitimate communication parties Alice and Bob is greater than that of $\lambda/2$ (λ is the carrier wavelength). At this point, the legitimate channel and the eavesdropping channel are independent of each other, i.e. Eve cannot obtain any channel information of Alice and Bob.

In the second case, Eve is close to Alice or Bob, which indicates that the distance is less than that of $\lambda/2$. Therefore, h_{AB} can be considered to have a certain correlation with h_{AE}. Eve can obtain information about the legitimate channel h_{AB} from the eavesdropping channel h_{AE}.

We use the frequency domain of the wireless channels to extract the phase information as the initial value of the chaotic sequence. 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, i.e., $h_{AB} = h_{BA}$ is guaranteed. In addition, all signals used in this algorithm are frequency domain signals.

B. DIGITAL ENCRYPTION METHOD BASED ON CHAOTIC SEQUENCE

The chaotic system is a typical nonlinear dynamic system, which is considered as an important pseudo random source generator. Due to its characteristics such as initial value sensitivity and irreversibility, the system has attracted wide attention. We compare the characteristics of chaotic systems and traditional encryption methods, as shown in Fig. 3. In comparison with the traditional encryption method, the chaotic encryption scheme does not require multiple rounds of iteration, which is more rapid and simple for practical implementation.

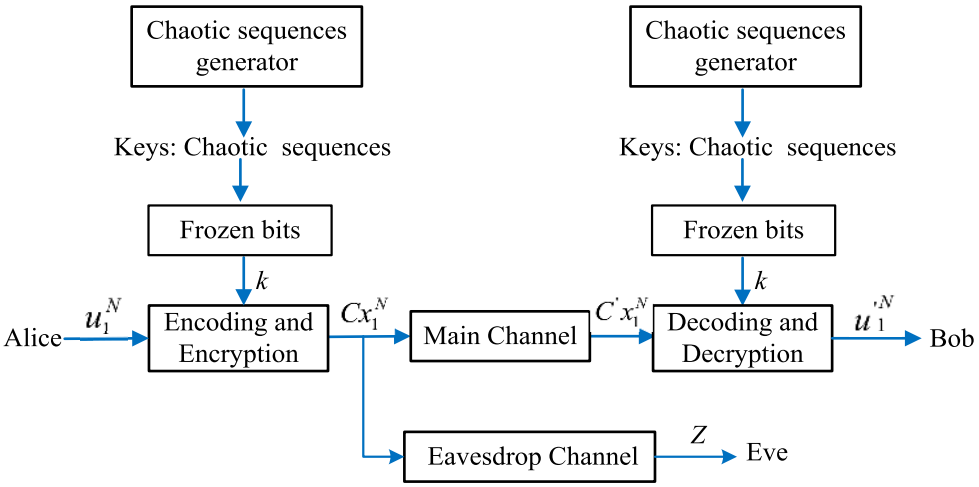


FIGURE 4. The physical layer encryption model of chaotic sequences transmission based on frozen bits of polar codes.

There are three types of chaotic dynamics models including discrete chaotic mapping system, continuous chaotic system and hyper-chaotic system. In general, discrete chaotic real value sequences are generated from the discrete chaotic mapping systems and then quantified to digital chaotic binary sequences by appropriate quantification methods. The typical discrete chaotic system is a Logistic map, and the chaotic system used in this paper is also the Logistic map. The Logistic map is the most commonly used one-dimensional chaotic map derived from the evolution of the insect population model [22]. The chaotic sequences used in this paper are generated by Logistic map. The map equation is:

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

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).

III. CHAOTIC SEQUENCES USED IN FROZEN BITS

A. SYSTEM OVERVIEW

The system diagram of our proposed algorithm is shown in Fig. 4. It is shown that the transmitter Alice sends messages to Bob while Eve wants to get the transmitted message. Alice and Bob have the same keys k. When Alice transmits the messages to Bob, the ciphertext will be obtained after the plaintext is encoded and encrypted in the module of Encode and Encryption. Bob receives the ciphertext, and then decodes and decrypts it in the module of decoding and decryption to get the message. The encryption and the coding which used polar codes are implemented in the physical layer. Encoding and encrypting are implemented at the same time in the module. Besides, the sequences are generated by chaotic sequences generator and stored in the frozen bits of the polar codes. Since what Eve gets should be the encrypted ciphertext Z which is out of order, it will be more difficult for Eve to decode and the security of the system can be enhanced.

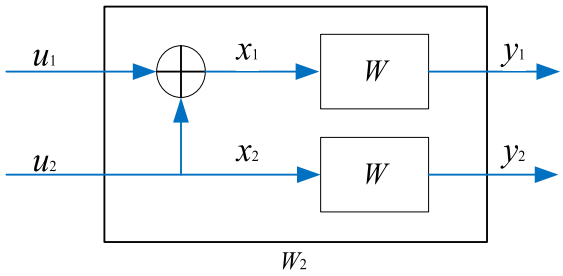


FIGURE 5. Channel W_2.

B. CODING AND DECODING OF POLAR CODE

First, we give a brief introduction of polar code. Assuming W is a B-DMC, a vector channel $W_N : X^N \rightarrow Y^N$ will be obtained if N independent channel W are combined in a certain way, where $N = 2^n$ and $n \geq 0$. The iteration starts at level-0, two independent channels are combined as shown in Fig. 5. The transition probability is

$$W_2\left(y_1, y_2 | u_1, u_2\right) = W\left(y_1 | u_1 \oplus u_2\right) W\left(y_2 | u_2\right) \tag{2}$$

In the recombined channel W_2, the input message is u_1^2 which means u_1 to u_2, and the recombined information bits is denoted by x_1^2 which means x_1 to x_2. The recombination of channels is shown as Fig. 5, and it can be denoted as:

$$x_1^2 = u_1^2 \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = u_1^2 G_2 \tag{3}$$

This can be deduced to the channel W_N as shown in Fig. 6. The recursive expression of any generator matrix can be derived, and the generator matrix G_N is defined as

$$G_N = B_N F^{\otimes \log_2 N} \tag{4}$$

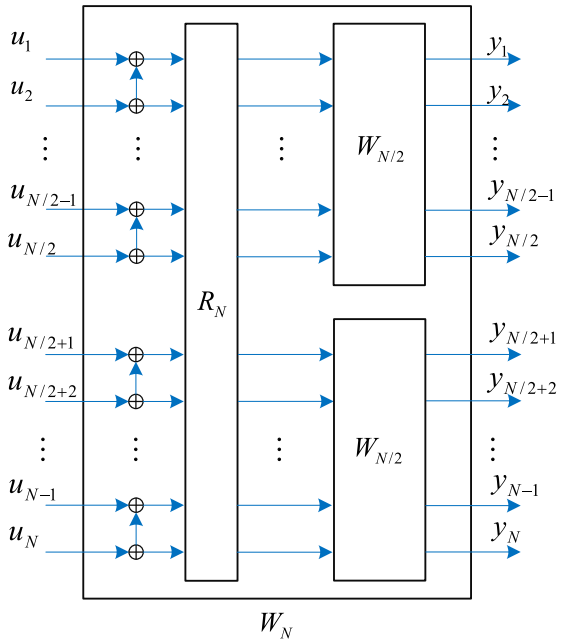


FIGURE 6. Channel W_N.

where $F = G_2$, $\otimes$ is inner product [22] and B_N is a bit-reversal permutation matrix [3].

The information set is an index set of the information channel, and the quality of the channel is mainly measured by Bhattacharyya parameters. The information bit selection methods for different channels are different. The additive white Gaussian noise channel (AWGN) is a channel whose noise is subject to the Gaussian distribution with σ^2 as its variance and 0 as its mean in this paper. The definition of the Bhattacharyya Parameter is as follows [5]:

$$\begin{aligned} Z(W) &= \int_{-\infty}^{+\infty} \sqrt{W(y|0)\, W(y|1)}\, dy \\ &= \int_{-\infty}^{+\infty} \sqrt{\frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y-1)^2}{2\sigma^2}} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y+1)^2}{2\sigma^2}}}\, dy \\ &= e^{-\frac{1}{2\sigma^2}} \end{aligned} \tag{5}$$

The encoding of polar code is the same as the general linear block codes. The sequence u_1^N to be encoded consists of the information bits u_A and the frozen bits u_{A^c}. While encoding, $u_A G_N(A)$ will be achieved after G_N and the rows that correspond to the element in set A are encoded, and $u_{A^c} G_N(A^c)$ will be achieved after the rest rows and fixed bits are encoded. The encoded word x_1^N of polar code is

$$x_1^N = u_1^N G_N = u_A G_N(A) \oplus u_{A^c} G_N\left(A^c\right) \tag{6}$$

The encoding method can be defined by the parameter vector (N, K, A, u_{A^c}), where$N$ is the code length, K represents the length of the information bits, the ratio K/N denotes the code rate, A is the set of information bits and u_{A^c} is composed of non-information elements known as the frozen bits.

A successive cancellation (SC) decoder is applied in this paper, which is a hard decision algorithm by calculating the likelihood ratio (LR) information of the bit channel iteratively. Besides, the LR information of W_N^i can be represented as:

$$L_N^i(y_1^N, \hat{u}_1^{i-1}) = \log \frac{W_N^i(y_1^N, \hat{u}_1^{i-1}|0)}{W_N^i(y_1^N, \hat{u}_1^{i-1}|1)} \tag{7}$$

The decision rule in this work can be shown as

$$\hat{u}_i = \begin{cases} u_i, & i \in A^c \\ h_i(y_1^N, \hat{u}_1^{i-1}), & i \in A \end{cases} \tag{8}$$

where $\{u_i, i \in \mathcal{A}^c\}$is frozen bit, then

$$h_i(y_1^N, \hat{u}_1^{i-1}) \triangleq \begin{cases} 0, & L_N^i(y_1^N, \hat{u}_1^{i-1}) \geq 1 \\ 1, & otherwise \end{cases} \tag{9}$$

The decoder focuses on calculating the transition probability and the LR of each bit channel.

C. TRANSMISSION OF CHAOTIC SEQUENCES IN FROZEN BITS

The chaotic sequences are generated by a chaotic system. Compared with traditional encryption methods, the chaotic encryption scheme does not need rounds of iterations, which could implement the encryption method rapidly and easily. In this paper, a typical method of discrete chaotic system Logistic mapping [21] is used to meet the requirements of the encryption communication system for key sequences. As for the encoder, the information bits vector u_1^N consists of a random part u_A and a fixed part u_{A^c} which are frozen bits. After this point, the code-word x_1^N can be obtained. Besides, the channel will be a good channel and transfer useful information when $i \in A$ whereas it will be a bad channel and not transfer useful information when $i \in A^c$. The frozen bits which are stored in polar codes are known to the receiver when decoded. So the frozen bits are wasted in traditional methods.

In this paper, Logistic discrete chaotic mapping system is used to generate discrete chaotic sequences, and then these sequences will be quantized into digital chaotic binary sequences based on appropriate quantization method. Meanwhile, the bad channel in the encoding will be used to transfer the chaotic sequences, which indicates the security will be enhanced after placing the chaotic sequence in the frozen bits.

Taking of code length $N = 8$ of polar codes as an example. As shown in Fig. 7, Q_1, Q_2, Q_3, Q_4 are chaotic sequences which are stored in frozen bits. At this point, the frozen bits of polar codes in (6) are no longer the full zero sequences, but the chaotic sequences. The encoding process can be describe as

$$x_1^N = u_1^N G_N = u_A G_N(A) \oplus k G_N\left(A^c\right) \tag{10}$$

where k is the chaotic sequence. Similarly, in the process of SC decoder in (8), the frozen bits $\{u_i, i \in \mathcal{A}^c\}$ are also chaotic

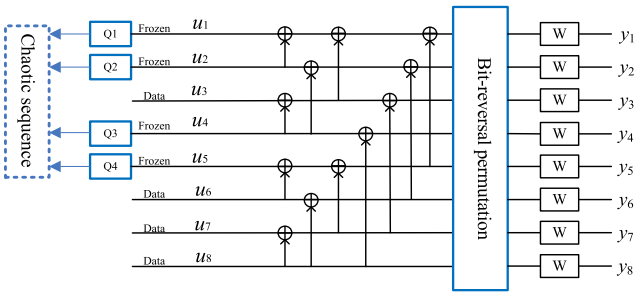


FIGURE 7. Adding the chaotic sequence on frozen bits.

sequences Q_i.

$$\hat{u}_i = \begin{cases} Q_i, & i \in A^c \\ h_i(y_1^N, \hat{u}_1^{i-1}), & i \in A \end{cases} \tag{11}$$

The chaotic sequences, which are stored in frozen bits, need to recurse in the process of decoding. Because Eve does not know the value of chaotic sequences, the decoding error will be caused in the process of decoding.

IV. A DELAYED FEEDBACK CHAOTIC ENCRYPTION ALGORITHM BASED ON WIRELESS CHANNEL CHARACTERISTICS

A. A CHAOTIC SEQUENCE GENERATION ALGORITHM BASED ON WIRELESS CHANNEL CHARACTERISTICS

Due to the wireless channel characteristics of the space-time uniqueness, short-time reciprocity and the time-variability, it is possible to generate the key based on the channel characteristics. By using the CSI as the public random source, both parties of communication detect the channel characteristics. By using the channel characteristics as the key source for quantification, information reconciliation, privacy amplification, etc., the same key is finally generated for generation of chaotic sequences. The chaotic sequences are used in encryption and decryption of the channel code information. In this paper, the characteristics of the wireless channel are used for extracting the binary sequence and converting the sequence into the chaotic system initial value; the algorithm process is as follows:

1) Extraction of binary sequence key based on the characteristics of the wireless channel : $\{r_i | i = 1, 2, \ldots, k\}$.

2) Conversion of the binary sequence to the initial value of chaotic sequence : $\{x_1 = \sum_{i=1}^{k} r_i 2^{-i}\}$

In practical implementations, the initial value of chaotic sequence need to be generate according to the accuracy requirements. Then we transform the sequence to the required initial value of the chaotic sequence according to the algorithm; and finally select a suitable chaotic mapping algorithm to generate chaotic sequence values.

B. THE PROCESS OF SYSTEM ENCRYPTION AND DECRYPTION

The system encryption process is shown in Fig. 8. The data stream is divided into k bits for a set of $M_i, i = 1, 2, 3 \ldots$ The plaintext sequence M_i and the chaotic sequences Q_i are XORed to obtain P_i,

$$P_i = M_i \oplus Q_i \tag{12}$$

P_i is coded by polar code sequence under the action of a generator matrix G to obtain codeword U_i.

$$U_i = P_i G = (M_i \oplus Q_i)G \tag{13}$$

P_i is stored in a register and after a delay of one time unit, the obtained P_i and the encoded code sequences U_i (which is obtained through the encryption module E are XORed to obtain the ciphertext C_i.

$$C_i = P_{i-1} \oplus U_i = P_{i-1}(M_i \oplus Q_i)G \tag{14}$$

The first plaintext module U_1 is XORed with the initial sequence P_0 which is the chaotic sequence of a chaotic system. It should be noted that since the bit length changes after U_i is encoded, the length of U_i is different from that of P_{i-1}, and thus the XOR operation of equation (14) needs to be designed based on the coding bit rate. Taking the code rate 1/2 as an example, when the XOR happens to (14), U_i needs to be divided into two groups, and let each group XOR with P_{i-1} to obtain the ciphertext C_i.

As shown in Fig. 8, the decryption process corresponds to the encryption process. It is assumed that the legitimate receiver extracts the same key, so the same chaotic sequence Q_i and initial sequence P_0 are generated. The ciphertext C_i goes through the noisy channel. The error vector introduced by the channel is Z_i and Z_i is in the range of error correction. Then

$$C_i' = C_i \oplus Z_i \tag{15}$$

From (14), we know that:

$$C_i' = P_{i-1} \oplus U_i = P_{i-1} \oplus (M_i \oplus Q_i)G \oplus Z_i \tag{16}$$

C_i' is XORed with P_{i-1} to get code word U_i',

$$\begin{aligned} U_i' &= C_i \oplus P_{i-1} \\ &= P_{i-1} \oplus (M_i \oplus Q_i)G \oplus Z_i \oplus P_{i-1} \\ &= (M_i \oplus Q_i)G \oplus Z_i \end{aligned} \tag{17}$$

The first received ciphertext is XORed with the initial sequence P_0. P_0 is a chaotic sequence generated by a chaotic system. Note that the XOR operation here is the same as in (14) and is related to the code rate. Similarly, taking the code rate 1/2 as an example in (17), it is necessary to divide C_i into two groups firstly. Then each group is respectively XORed with P_{i-1} to obtain the code word U_i' (which is completed in the encryption module E). Sequence P_i is obtained after U_i' is channel-decoded through SC decoder. Since Z_i is within the error correction range of channel coding, P_i is XORed with the chaotic sequence Q_i to obtain the plaintext M_i'.

$$\begin{aligned} M_i' &= P_i \oplus Q_i \\ &= M_i \oplus Q_i \oplus Q_i \\ &= M_i \end{aligned} \tag{18}$$

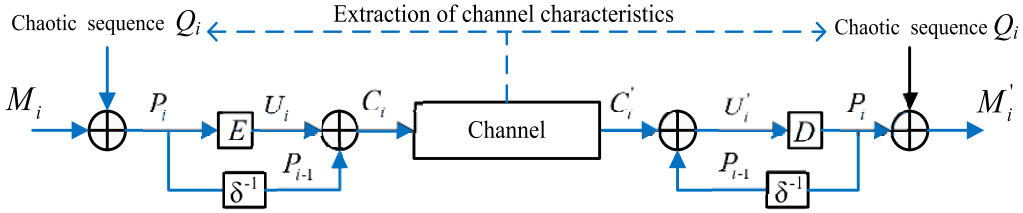


FIGURE 8. Encryption and decryption module based on chaotic sequence.

In this system, the signal is randomly processed twice before and after the channel coding in the physical layer. This confuses the code word before and after coding. Different from the general randomization operation, this algorithm uses the chain effect of delayed feedback, so that the randomization is not only reflected in each group but also spread to multiple groups, resulting in different transformation sequences in the same information group and increasing the difficulty of cryptanalysis.

This algorithm not only recovers the error correcting performance of the error correction code, but also can make full use of the wireless channel feature of the physical layer to extract key. Besides, it realizes the encryption protection of the encoded information and achieves secure communication under the premise of requiring a small number of keys.

V. PERFORMANCE EVALUATION AND SIMULATION VERIFICATION

A. RELIABILITY AND SECURITY ANALYSIS OF THE SCHEME CHAOTIC SEQUENCES USED IN FROZEN BITS

Polar encoding and SC decoder are adopted in this paper. The number of frozen bits are dependent on the code length and code rate. As shown in Fig. 9 and Fig. 10, the frozen bits in the encoding process do not contribute to the reliability because they are not related to the calculation of the bit error rate (BER). However, the code length and code rate have a certain influence on the error performance of polar code. The effect of polarization is more obvious when the value of code length N increases, and the Bhattacharyya Parameter Z of the channel selected to transmit information will be smaller, so the BER decreases. For the code rate R, when R increases, the number of channels selected to transmit information also increases. Meanwhile, the poor channels will be added, resulting in the increasing of BER.

Typically, to encrypt the keys, both the sender and the receiver will use the same sequence to encrypt and decrypt the plaintext. In the encoder process of polar codes from (6), the chaotic sequences are stored in frozen bits and the chaotic sequences k are placed in A^c. u_A and $\tilde{u}_A$ are information sequences in two transmissions. x_1^N and $\tilde{x}_1^N$ are coding sequences from two transmissions. If the chaotic sequences stay unchanged as shown in (19), which means $k_1 = k_2$. Then the impact of the sequence k which appeared in x_1^N and $\tilde{x}_1^N$ will be offset through simple math calculation. So the security of the system cannot be guaranteed if the sequence

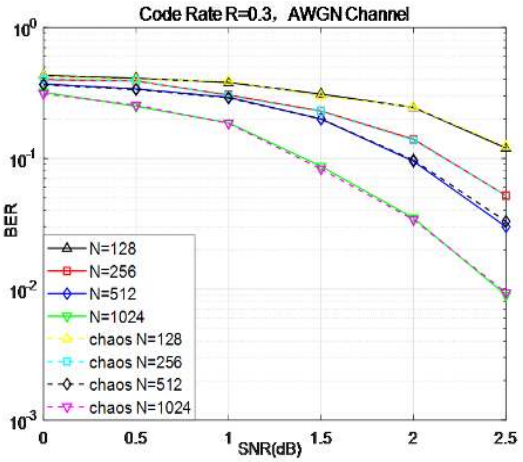


FIGURE 9. The BER performance of the system with the chaotic sequence in the frozen bits with different code lengths.

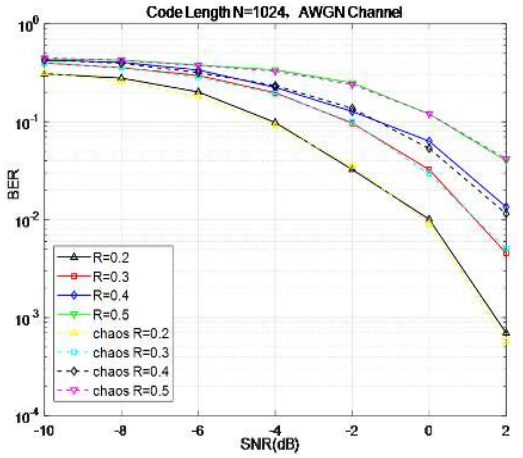


FIGURE 10. The BER performance of the system with the chaotic sequence in the frozen bits with different code rates.

stays unchanged. Besides, Eve can unscramble the original information as long as they intercept the coding sequence twice in the channel.

$$\begin{aligned} x_1^N &= u_1^N G_N = u_A G_N(A) \oplus k_1 G_N\left(A^c\right) \\ \tilde{x}_1^N &= \tilde{u}_1^N G_N = \tilde{u}_A G_N(A) \oplus k_2 G_N\left(A^c\right) \end{aligned} \tag{19}$$

In this paper, Alice and Bob generate the same chaotic sequence through a chaotic sequences generator. Eve can obtain chaotic sequences containing large BER from frozen bits by some methods. However the chaotic sequence is time

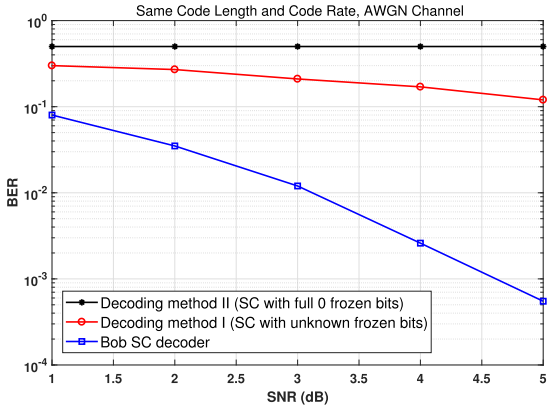


FIGURE 11. The BER performance of several decoding methods.

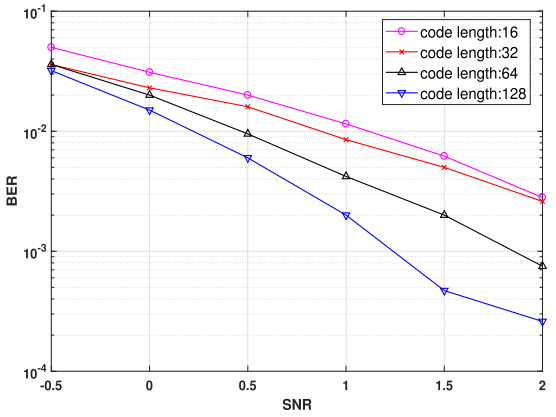


FIGURE 12. Comparison of the BER performance of the polar codes in the chaotic encoding and encryption system.

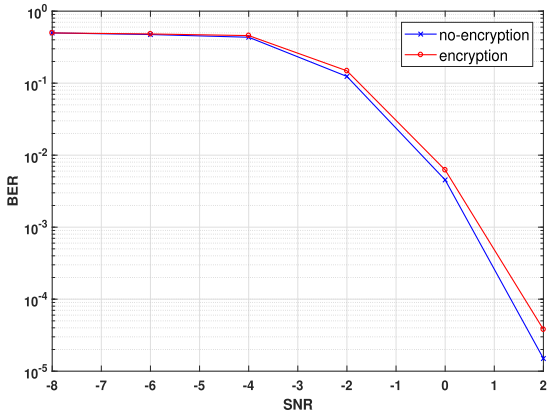


FIGURE 13. Simulated comparison of the effect of chaotic encryption on BER performance.

varying. Since each frame is different, Eve cannot get legal information even if it obtains chaotic sequences with errors. It is worth noting that if the signal noise ratio (SNR) of the eavesdropping channel is very high (above 10 dB); it may cause leakage of large chaotic sequences information. Therefore, this method needs to cooperate with other physical layer security methods which can be used to reduce the SNR of eavesdroppers in practical applications, such as artificial noise, MIMO beamforming, etc. [12]–[14]. Besides, according to the principle in the algorithm and the system requirements, if the code rate or code length of polar code varies, the length of the chaotic sequence based on the chaotic sequence could be extended, which can increase the key space of the system and make it more difficult for Eve to decrypt the ciphertext.

Based on the previous discussion, it is reasonable to assume that the eavesdropper does not have the knowledge of chaotic sequences. We consider that Eve can use the following decoding methods:

1) The eavesdropper regards the frozen bits which are used to store the chaotic sequence as an all-zero sequence and then uses SC decoder.

2) The eavesdropper regards the frozen bits which are used to store the chaotic sequence as unknown bits and then uses SC decoder.

The BER simulation results of several decoding methods are shown in Fig. 11. Decoding method-I or Decoding method-II is the method that Eve decodes the frozen bits directly as an all-zero sequence and then employs the SC decoder, or treats the frozen bits as an unknown bits and then employs the SC decoder, respectively. Bob SC decoder in Fig. 11 is the method that the receiver decodes and decrypts the information through SC decoder. We can see the bits error rate will increase greatly no matter what kind of decoding methods Eve uses.

B. RELIABILITY AND SECURITY ANALYSIS OF THE DELAYED FEEDBACK CHAOTIC ENCRYPTION ALGORITHM

In the AWGN channel, the influence of the length of the polar code on the system performance is analyzed through simulation. We also consider the BER performance of the proposed methods. The simulation results are shown in Fig. 12 and Fig. 13.

It can be seen in Fig. 12 that in the chaotic encoding and encryption system, the code length of the polar code affects the BER performance. The polar codes with longer code length have better BER performance than the polar codes with longer code length. When the code length increases, the effect of polarization is more pronounced. Besides, from the simulation results shown in Fig. 13, we can see that the chaotic encoding and encryption has almost no influence on the reliability of the system and guarantees the error correction performance of the error-correcting code.

Eve can deduce the channel-coding scheme of communication between Alice and Bob if he has the same receiving capability as the legitimate communicator. Ever can perform computational attacks with powerful computing. We assume that Eve knows the process of the equivalent channel characteristics information and the channel coding method. In other words, the security of the system does not depend on the confidentiality of the algorithm.

1) IMPACTS OF IMPERFECT CSI

Due to influences such as the channel noise, detection error, and imperfect CSI, there may exist inconsistent information bits in the initial key. Therefore, we need an information reconciliation process to make the keys consistency. Zhang *et al.* [42] proposed practical design guidelines on secure key generation systems. The work in [43] investigated and quantified channel measurements' cross-correlation relationship affected by noise and non-simultaneous measurements. So Alice and Bob can eliminate the influence of imperfect CSI through information negotiation. The existing information negotiation methods include Cascade method [36], binary search method [44] and error correcting code methods [37]–[39].

2) CONDITIONS OF KEY GENERATION METHODS

The key generation method is based on the fact that the legitimate communication parties detect the wireless channel during the coherence time, and then perform quantification, information negotiation and security enhancement of the channel characteristic observed values to extract a secure shared key. The wireless channel can be used as a natural random source to extract keys. The conditions of key generation methods are as follows:

Short-Term Reciprocity: According to the propagation characteristics of electromagnetic waves, in the TDD communication mode, the fading experienced by the uplink and downlink signals during the coherence time are the same, ensuring that both parties of legitimate communication can extract the consistent channel characteristics during one channel coherence time.

Time-Variability: In reality, the wireless environment is complex and changeable. Therefore, the wireless channel is unpredictable and random. The legitimate communication parties generate different keys in different periods in order to realize real-time update of the keys, making it possible to have one key at a time.

Space-Time Uniqueness: The eavesdropper cannot obtain the same channel characteristics as the legitimate user, nor can it extract the same key as the legitimate user. We assume that the distance between Eve and Alice or Bob is at least $\lambda/2$, and the keys extracted by Alice and Bob over the wireless channel are not related to Eve. Hence, Eve cannot get the same binary key. In addition, the chaotic system is very sensitive to the initial value, so Eve cannot decipher the ciphertext sequence.

3) KEY RANDOMNESS ANALYSIS

A good security encryption strategy requires strong key sensitivity, which indicates that the eavesdropper cannot restore the source information when there is a very small difference between the keys. We use the C++ high-level programming language and the GNU multiple precision arithmetic library (GMP) to test the sensitivity of the chaotic system to the initial values. The test results are shown in table 1.

TABLE 1. Sensitivity detection results of logistic chaotic sequence key.

Key difference accuracy	Chaos sequence differences
10^{-10}	50.06%
10^{-20}	49.97%
10^{-30}	50.14%
10^{-40}	49.91%
10^{-50}	49.72%

After several tests, it is found that when the initial value x_n of the two keys is randomly selected between (0, 1), the difference is 10^{-10}, and the generated chaotic sequence difference rate is around 50%. There are half difference in chaotic sequences which are generated by two seed keys. Eve cannot decipher the received ciphertext information, i.e., the algorithm has high key precision and strong key sensitivity.

4) KEY SPACE ANALYSIS

Due to the randomness of the wireless channel, the extracted characteristic key has no correlation, and Eve cannot get any statistical information from it but violently crack the key by exhaustive methods. It is assumed that except the key extracted by the channel characteristics are completely confidential, all other keys are open, including the chaotic sequence generation principle, the coding mode, and the system encryption and decryption principle, etc. If the bit key length of the key is 128 bits, and the key space of the system is 2^{128}, so the key space is very large, which makes it very difficult to crack the information of the algorithm by exhaustive methods. In addition, based on the principle of the algorithm, the bit key length can be extended according to the system requirements, to increase the key space of the system and make it harder for eavesdroppers to decipher.

VI. CONCLUSION

We propose a physical layer encryption algorithm of chaotic key transmission based on frozen bits of polar codes. Chaotic sequences are allocated in the frozen bits of polar codes. The placement of the chaotic sequence with frozen polar bits has no effect on reliability for the receiver. The key space is large enough to prevent the brute-force attack. We consider different decoding methods for Eve, and Eve has high BER in all methods.

To further improve the security, we improve the algorithm. The legal parties extract the binary sequence key through the wireless channel and convert it into the initial value of the chaotic system to generate a chaotic sequence with a certain length, which is used to encrypt the encoded information. This algorithm has strong key sensitivity and large key space. The proposed algorithm not only ensures the error correction performance of the system but also enhances the security performance of the system. It has a wide application prospect in the future 5G commercial communication systems and military communication systems.

VII. ACKNOWLEDGMENT

This paper will be presented in part at the 2018 IEEE International Conference on Electronics and Communication Engineering [28].

REFERENCES

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[2] E. Arikan, "Channel combining and splitting for cutoff rate improvement," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 628–639, Feb. 2006.

[3] 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.

[4] S. B. Korada, E. a o lu, and R. Urbanke, "Polar codes: Characterization of exponent, bounds, and constructions," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6253–6264, Dec. 2010.

[5] H. Li and J. Yuan, "A practical construction method for polar codes in awgn channels," in *Proc. IEEE Tencon-Spring*, Sydney, NSW, Australia, Apr. 2013, pp. 223–226.

[6] A. H. A. El-Malek, A. M. Salhab, and S. A. Zummo, "New bandwidth efficient relaying schemes in cooperative cognitive two-way relay networks with physical layer security," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5372–5386, Jun. 2017.

[7] 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.

[8] W. Hao, L. Yin, and Q. Huang, "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.

[9] N. Ghose, B. Hu, Y. Zhang, and L. Lazos, "Secure physical layer voting," *IEEE Trans. Mobile Comput.*, vol. 17, no. 3, pp. 688–702, Mar. 2018.

[10] G. Chen, J. P. Coon, and M. D. Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.

[11] A. Kharel and L. Cao, "Analysis and design of physical layer raptor codes," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 450–453, Mar. 2018.

[12] 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.

[13] S. Wang, W. Li, and J. Lei, "Physical-layer encryption in massive MIMO systems with spatial modulation," *China Commun.*, vol. 15, no. 10, pp. 159–171, Oct. 2018.

[14] W. Stallings, "Cryptography and network security: Principles and practice," *Int. J. Eng. Comput. Sci.*, vol. 1, no. 1, pp. 121–136, Jan. 2011.

[15] T. Hwang and T. R. N. Rao, "Secret error-correcting codes (SECC)," in *Proc. Int. Cryptol. Conf. Adv. Cryptol.*, Aug. 1988, pp. 362–367.

[16] 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, Jul. 2018.

[17] A. Payandeh, M. Ahmadian, and M. R. Aref, "Adaptive secure channel coding based on punctured turbo codes," *IEE Proc.-Commun.*, vol. 153, no. 2, pp. 313–316, Apr. 2006.

[18] R. J. Mceliece, "A public-key cryptosystem based on algebraic coding theory," *Deep Space Netw. Prog. Rep.*, vol. 44, pp. 114–116, Jan./Feb. 1978.

[19] O. Adamo, S. Fu, and M. R. Varanasi, "Physical layer error correction based cipher," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Miami, FL, USA, Dec. 2010, pp. 1–5.

[20] O. E. Rössler, "An equation for continuous chaos," *Phys. Lett. A*, vol. 57, no. 5, pp. 397–398, Jul. 1976.

[21] M. Hénon, "A two-dimensional mapping with a strange attractor," *Commun. Math. Phys.*, vol. 50, no. 1, pp. 69–77, Feb. 1976.

[22] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, Jun. 1976.

[23] M. J. Feigenbaum, "Quantitative universality for a class of nonlinear transformations," *J. Stat. Phys.*, vol. 19, no. 1, pp. 25–52, Jul. 1978.

[24] P. Chen, Y. Fang, G. Han, and G. Chen, "An efficient transmission scheme for dcsk cooperative communication over multipath fading channels," *IEEE Access*, vol. 4, pp. 6364–6373, 2016.

[25] P. Chen, Y. Fang, K. Su, and G. Chen, "Design of a capacity-approaching chaos-based multiaccess transmission system," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10806–10816, Dec. 2017.

[26] P. Chen, L. Shi, Y. Fang, G. Cai, L. Wang, and G. Chen, "A coded dcsk modulation system over Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 3930–3942, Sep. 2018.

[27] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[28] L. J. Lu, P. Z. Xinjin, and L. Wei, "A delayed feedback chaotic encryption algorithm based on polar code," in *Proc. IEEE Int. Conf. Electron. Commun. Eng.*, Xi'an, China, Dec. 2018.

[29] A. Rahmanpour, V. T. Vakili, and S. M. Razavizadeh, "Enhancement of physical layer security using destination artificial noise based on outage probability," *Wireless Pers. Commun.*, vol. 95, no. 2, pp. 1553–1565, Jul. 2017.

[30] L. Cheng, W. Li, D. Ma, J. Wei, and X. Liu, "Moving window scheme for extracting secret keys in stationary environments," *IET Commun.*, vol. 10, no. 16, pp. 2206–2214, Nov. 2016.

[31] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual ofdm subcarrier's channel response," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842–1852, Sep. 2013.

[37] 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.

[38] H. Liu, J. Yang, Y. Wang, Y. J. 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.

[39] 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 14th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Orlando, FL, USA, Oct. 2017, pp. 46–54.

[40] D. Chen *et al.*, "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.

[41] 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*, Shanghai, China, Apr. 2011, pp. 1422–1430.

[42] 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.

[43] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *Proc. IEEE 17th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jul. 2016, pp. 1–5.

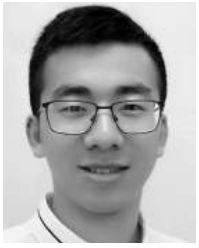
[44] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

XINJIN LU received the B.Sc. degree in communication engineering from Hunan University, 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.

JING LEI received the B.Sc., M.Sc., and Ph.D. degrees from the National University of Defense Technology, 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, National University of Defense Technology, and also 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.

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 currently 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.

KE LAI received the B.Sc. degree in communication engineering from the National University of Defense Technology, Changsha, 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 advanced multiple access techniques, channel coding, and physical layer security.



ZHIPENG PAN received the B.S. and M.S. degree in information and communication engineering from the National University of Defense Technology, 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.