IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 12, 2019, accepted April 28, 2019, date of publication May 3, 2019, date of current version May 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914720

Cryptographic Primitives and Design Frameworks of Physical Layer Encryption for Wireless Communications

WEI LI[1], (Member, IEEE), DES MCLERNON[2], (Member, IEEE), JING LEI[1], (Member, IEEE), MOUNIR GHOGHO[2,3], (Fellow, IEEE), SYED ALI RAZA ZAIDI[1], (Member, IEEE), AND HUAIHAI HUI[2], (Member, IEEE)

[1]Department of Communication Engineering, College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China
[2]School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, U.K.
[3]Department of Computer Science, International University of Rabat, Rabat 51555, Morocco

Corresponding authors: Wei Li (liwei.nudt.cn@gmail.com) and 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 Hunan Natural Science Foundation under Grant 2018JJ3609, in part by the U.K. British Council (Newton Fund) through the project "Wireless Sensor Networks for Real Time Monitoring of Water Quality" under Grant IL3264631003, and in part by the Research England Global Research Challenges Fund.

ABSTRACT Security is always an important issue in wireless communications. Physical layer encryption (PLE) is an effective way to enhance wireless communication security and prevent eavesdropping. Rather than replacing cryptography at higher layers, PLE's benefit is to enable using lightweight cryptosystems or provide enhanced security at the signal level. The upper cryptography is faced with a noise-free channel, and the processing object is bit data. In PLE, the effects of channel and noise can be exploited to enhance security and prevent deciphering. In addition, since the processing object is complex vector signals, there are more operational functions to select and design for PLE. The mathematical models, design frameworks, and cryptographic primitives of PLE are established. Two design frameworks are proposed: stream PLE and block PLE. For stream PLE, a new 3D security constellation mapping is derived. For block PLE, two types of sub-transforms are defined: isometry transformations and stochastic transformations. Furthermore, a practical system operation mode PLE-block chaining (PBC) is proposed to enhance the practical system security. The proposed PLE framework can resist known plaintext attacks and chosen-plaintext attacks. The simulation shows that the proposed isometry transformation method has good performances in terms of bit error ratio (BER) penalty and confusion degree.

INDEX TERMS Physical layer encryption, block PLE, stream PLE, isometry transformation, stochastic transformation, PLE-block chaining.

I. INTRODUCTION

Security is a serious problem in wireless communication systems due to the broadcast characteristics of wireless channels. In Shannon's pioneering work [1], security and reliability are considered and designed together. However, with the development of modern cryptography, security has become a research direction separate from communication design. While modern cryptography considers the encryption problem in error-free channels, communication system design considers transmission reliability and effectiveness. In a practical communication systems, such as the fourth-generation (4G) cellular standard and wireless LAN communication, the physical layer and the security layer are designed separately and so do not have much overlap with each other.

The emergence of physical layer security (PLE) technology combines the communication physical layer and the security layer. Wyner's original research took into account the secure transmission issues in noisy channels [2]. We call this *information-theoretic security*. This is a different way from up-layer cryptography. After Wyner's work, important research about PLS has been carried

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

out, including multi-antenna beamforming [3]–[5], artificial noise techniques [6]–[9], and cooperative interference techniques [10], to name but a few. Over the last two decades, researchers have developed a significant number of mathematical theories, technologies, algorithms, and solutions for information theory based PHY-security challenges. Based on information theory, PLS is designed to achieve security through secure coding which does not require keys. The problem faced by PLS is that it depends on the channel. When the security capacity is zero, that is, the eavesdropping channel is better than the legal channel, or if the eavesdropping channel is unknown, security cannot be guaranteed. Therefore, it is necessary to find other ways to enhance security at the physical layer.

Unlike the above PLS works, physical layer encryption (PLE) is another way to achieve security at the physical layer. PLE is a kind of security based on computational complexity, which needs to distribute keys on both the transmitter and receiver. The PLE system has no strict requirements on the number of antennas or channel conditions, and thus is more practical and can be applied to various types of wireless communication systems. Compared with traditional cryptography (that only considers perfect channels) it can take advantage of the effects of the channel and noise and provide security at the signal level rather than at the bit level. Rather than replacing cryptography at higher layers, one of PLE's benefits is to enable using lightweight cryptosystems, an important issue in devices with limited resources. Researchers considered PLE in a variety of communication systems including OFDM systems [11], [12], massive MIMO systems [13]–[15], Untrusted Relaying Systems [16], IEEE 802.15.4 protocols [17], rateless codes [18] and sparse code multiple access (SCMA) [19]. The work in [17] implemented a PLE system in ASIC and FPGA with low complexity and latency.

In general, the PLE technology has the following advantages:

1. Compared to PLS, PLE does not depend on the eavesdropper channel conditions. Even if eavesdroppers have more antennas and stronger reception capabilities, PLE can still guarantee secure transmission.

2. PLE has the characteristics of low latency. It also has low computational cost, so that the power consumption is small, the working time is long and the lifetime is suitable for application in the Internet of Things (IoT) network.

3. PLE provides enhanced security at the signal level. PLE operates in the complex signal domain, unlike traditional cryptography that only operates in the Boolean algebraic domain. Therefore, PLE has an enlarged ''operating space'', and more functions can be selected, which is conducive to the design and construction of a more secure encryption method.

4. PLE can introduce randomness functions that can be exploited against known plaintext attacks and linear attacks.

The main methods used in the existing PLE literatures are constellation rotation, subcarrier disturbance, symbol scrambling, training symbol reordering and so on. The above methods are based on the existing constellation modulation, and the output signal still leaks some information such as modulation. The output signal is not fully confused and may not be able to withstand known-plaintext attacks (KPAs) and chosen-plaintext attacks (CPAs) attacks.

In addition, the strict security definition of PLE is still lacking. Precise cryptographic primitive definitions and rigorous proofs of security are very important for building PLE-based practical cryptographic protocols. Rigorous proofs of security is one of the requirements for PLE schemes to be standardized.

In this paper, we will concentrate on the general mathematical model and framework of PLE, and consider how to define and measure the security of PLE. We will establish the cryptographic primitives of PLE and consider the basic design rules.

The main contributions of this paper are:

- According to different operating modes, we divide PLE into two categories: *stream PLE* and *blockPLE*. We will define *cryptographic primitives* for *stream PLE* and *block PLE*. Then we will give the definition of semantic security for PLE.
- We will propose *design frameworks* and the basic rules of both stream and block PLE.
- We will propose a new PLE function based on *isometry transformation*. We will define the *isometry transformation* and the *stochastic transformation* in block PLE. Isometry transformation can fully confuse multiple symbols while ensuring BER performance.
- In order to resist both KPA and CPA, a practical system operation mode PLE-block chaining (PBC) is proposed to enhance practical system security.
- We propose using the information entropy to measure the information leak and confusion degree of constellations, and propose design principles for the implementation of PLE.

The rest of the paper is organized as follows. The system model and security define is given is Section II. The design framework and rules of PLE are introduced in Section III. In Section IV, security analysis of KPA and CPA is discussed. Performance comparison and numerical simulations are given in Section V. Finally, Section VI summarizes the conclusions.

Note that this is an extended version of our previous conference paper [20]. The new contributions are summarized as follows: First, we give a semantic security define for PLE. Second, detailed proof that the isometry transformation will not change the bit error ratio (BER) performance of digital modulation constellations in Section III-B. Third, a practical system operation mode is proposed in Section III-C. Fourth, We give some design principles for implementation PLE in

TABLE 1. Comparison of PLE, PLS and cryptography.

	Key	Equivalent channel	Security	Operate domain
PLE	With key	Error channel	Computationally-secure; Takes use of the channel	Complex vector and bit space
Information theory based PLS	Without key	Error channel	Information theory-secure; Depends on channel	Complex vector
Cryptography	With key	Perfect channel	Computationally-secure	Bit level

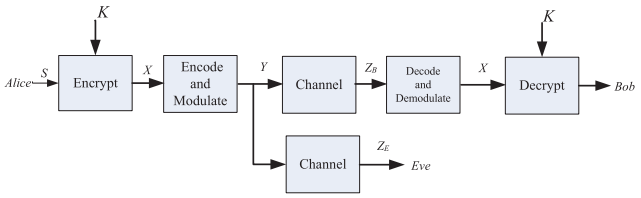

FIGURE 1. Traditional cryptography system model with encoding and modulation after encryption.

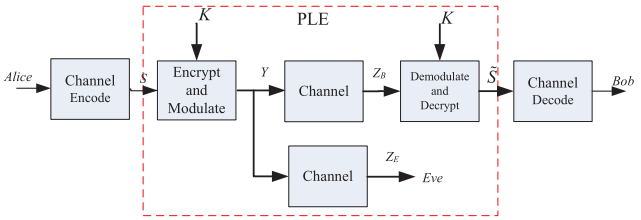

FIGURE 2. PLE communication system model.

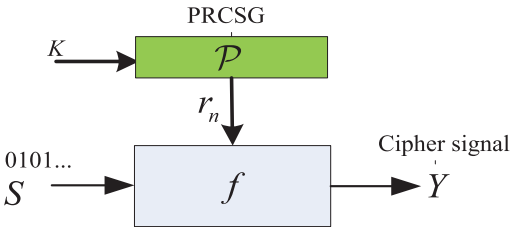

FIGURE 3. Stream PLE.

Section III-D. In Section IV, we present a more detailed security analysis. In addition, we give a design example and numerical simulations on a practical OFDM system in Section V.

Notation: $\mathbf{X}^T$, $\mathbf{X}^{-1}$, $\mathbf{X}^H$ and $\mathbf{X}^*$ denote respectively the transpose, inverse, conjugate transpose and conjugate of matrix $\mathbf{X}$. $\mathbf{I}_N$ denotes the N-dimensional identity matrix. $|x|$ is the absolute value of a complex scalar x. $\|\ldots\|$ denotes the Euclidean norm of a vector. $\mathbb{C}^n$ represents the space of $n \times 1$ vectors with complex elements. $\mathbb{C}^{m\times n}$ and $\mathbb{R}^{m\times n}$ represent the space of all $m \times n$ matrices with complex elements and real elements respectively. For sets $\mathcal{C}$ and $\mathcal{D}$, $\mathcal{C}\times\mathcal{D} = \{(c, d) \mid c \in \mathcal{C}$ and $d \in \mathcal{D}\}$, where $\times$ is the Cartesian product between two sets.

II. PLE SYSTEM MODEL AND CRYPTOGRAPHIC PRIMITIVE

A. COMPARISON BETWEEN PLE AND A TRADITIONAL CRYPTOGRAPHY SYSTEM

The main task of PLE and traditional cryptography is design a mapping from plaintext space to cipher signal space. The design requirement is that the legal receiver can easily recover the plaintext from the cipher signal, but the eavesdropper is infeasible to recover the plaintext. In order to better understand PLE, we compare the differences between PLE and traditional cryptography.

The structures of traditional cryptography and PLE are shown in Fig.1. and Fig.2, respectively. Fig.1. is a traditional cryptography system, where S is a plaintext sequence and a ciphertext X (binary sequence) is generated by the encryption algorithm based on the key K, and then sent to the channel by the coding modulation module. In the traditional cryptography system, we assumed that the encryption and decryption blocks experience a perfect channel. Error correction is guaranteed by the channel encoder/decoder module.

The system model of PLE is shown in Fig 2, where $\tilde{S}$ is the recovered plaintext which may contain errors. PLE also requires keys that needs to be sent from a secret channel in advance or extracted from wireless channels [21]–[24]. We can see that PLE is essentially a joint design of modulation and encryption. The PLE algorithm not only needs to consider security, but also needs to consider reliability and needs to combat the influence of channel and noise. Further, PLE needs to use the channel error to increase the difficulty of eavesdropper cracking. Furthermore, PLE deal with the complex signal which is different form the Boolean algebra based cryptography.

In Table 1, we summarize the differences between PLE, PLS, and cryptography. We can see that PLE is different from PLS and cryptography. We face new problems and need to propose new rules for PLE.

Then we consider two categories of PLE depending on the processing mode: Stream PLE and Block PLE.

B. STREAM PLE

Stream PLE uses the transmitted symbol as the basic encryption unit and can be considered as a time-varying encryption transform. The structure of stream PLE is shown in Fig.3., where $\mathcal{P}$ is a pseudorandom complex sequence generation function, r_n is a complex sequence, f is the encryption function. Stream PLE has the advantage of low latency and low error propagation. The disadvantages of stream PLE are: diffusion only inside the symbol and there is no overlap between the symbols. Next we give the detailed process of Stream PLE.

1) ENCRYPTION AND MODULATION

The pseudorandom complex sequences r_n (where n is the symbol index) are generated from the key K:

$$r_n = \mathcal{P}(K) = a_n + jb_n = A_n e^{\theta_n}. \tag{1}$$

Here, $\mathcal{P}$ is a pseudorandom complex sequence generation function. The function of r_n is used to change the transmitted symbols, making the output symbols confusing and randomly distributed. The distribution of r_n needs to be designed by the user.

Definition 1 [Pseudorandom Complex Sequence Generator (PRCSG)]: Consider ξ a probability distribution on $\mathbb{C}$ (a complex domain). We call a function $\mathcal{P} : \mathcal{K} \to \mathbb{C}^n$ (where $\mathcal{K}$ is the set of positive integers) a pseudo-random complex sequence generator if $\forall K \in \mathcal{K}, \quad \mathcal{P}(K) = \{r_1, r_2, r_3 \ldots\}$, where $\{r_n\}$ is a sequence of complex independent random variables which obeys the ξ distribution.

PRCSG is an algorithm for generating complex random sequences. But r_n is not a true random number because it is completely determined by the given initial key K.

The encryption function is:

$$Y_n = f(s_n, r_n). \tag{2}$$

The output encypted symbol sequence is $Y = \{Y_1, Y_2, \ldots\}$ whose nth element is Y_n (a complex number), and Y_n is a function of s_n and r_n. Here, $S = \{s_1, s_2, \ldots\}$ is the plaintext binary sequence to be sent. For M-ary modulation, s_n (the nth element of S) is a $\log_2 M$-length block of binary bits whose elements are "0" or "1".

There are two aspects to consider when designing an encryption function: first, it is easy for Bob (with K) to recover S; second, it is infeasible for Eve (without K) to find out S.

We will discuss in detail how design f functions in section III.

2) DEMODULATION AND DECRYPTION

In the PLE system, it is a joint decryption and detection process, unlike traditional communication systems, where decryption and detection are two separate processes.

The decryption and demodulation algorithm is denoted as:

$$\tilde{S} = \mathcal{D}(Z_B, K) \tag{3}$$

where $\mathcal{D}$ is the joint decryption and detection algorithm. When designing $\mathcal{D}$ we need to consider both reliability and complexity.

C. BLOCK PLE

Different from stream PLE, block PLE is only required to operate on plaintexts of a specific length. Block PLE maps fixed chunks of bits into complex vector signals. Here the mapping function can be random. Randomness can be against CPAs or KPAs.

Block PLE is modeled as a series of functions that map binary sequences to complex vectors according to the key K:

$$\mathbf{S} = \{s_1 s_2 \ldots s_l\} \xrightarrow{K} \mathbf{Y} = \{Y_1 Y_2 \ldots Y_N\} \tag{4}$$

where $\mathbf{S}$ is a binary message sequence of length l. K is the k_l bits key, and $\mathbf{Y} \in \mathbb{C}^{N\times 1}$ is the cipher signal vector. Different from stream PLE, l is a fixed large number (for example l= 256 or 512).

$\mathbb{F}_2$ is the finite field of two elements and F_2^l denotes the l length vector space elements in F_2. Then, the Block PLE in (4) can be represented as the following mapping T:

$$T : F_2^l \times F_2^{k_l} \to \mathbb{C}^N \tag{5}$$

Note that T is not necessarily a deterministic function and it also allows for the introduction of randomness.

We also can consider (5) as a family of functions with one parameter, and represent it as

$$\mathbf{Y} = T_K(\mathbf{S}).$$

The main job for PLE is to design the appropriate function T_K. Since the types of mapping functions are different, the design of PLE is quite different from traditional cryptography. From a mathematical point of view, the set of functions that can be selected is infinite. We have more function types to choose from and also have a larger key space to combat brute force.

We need to make the function T_K have a pseudo-random property, i.e., T_K (with a randomly-chosen key K) cannot be distinguished from and the function of random uniform selection with the same domain and value range.

D. CHANNEL MODEL

Returning to Fig.2, then after the cipher signal Y passes through the channel, the symbols received at the legal receiver and the eavesdropper are respectively: As shown in Fig.2 the cipher signal Y is transmitted to the wireless channel through the RF module. We use H_B and H_E to represent the channel functions (including the effects of noise) of Bob and Eve, respectively. The signals received by Bob and Eve are

$$Z_B = H_B(Y) \tag{6}$$

$$Z_E = H_E(Y). \tag{7}$$

E. DEFINITIONS OF CRYPTOGRAPHIC PRIMITIVES OF THE PLE SYSTEM

Our next work is to establish the cryptographic primitives of PLE. The cryptographic primitive is the basic unit for building a secure protocol. Only the definition of a clear cryptographic primitive can guide the design of PLE and further apply PLE to the actual security standards.

The *cryptographic primitives* of PLE is defined as follows:

Definition 2: (Physical Layer Encryption System):

Message space $\mathcal{M}$: the set of all possible plaintext messages, a finite set. All input messages $S \in \mathcal{M}$.

Cipher signal space $\mathcal{C}$: the set of all possible ciphers. All cipher signals $Y \in \mathcal{C}$.

Key space $\mathcal{K}$,$\mathcal{K}'$: possible encryption key set $\mathcal{K}$, and possible decryption key set $\mathcal{K}'$. For the symmetric PLE, $\mathcal{K}$=$\mathcal{K}'$.

The encryption key K is chosen from $\mathcal{K}$, and the decryption key K' is chosen from $\mathcal{K}'$, and so $K \in \mathcal{K}$, $K' \in \mathcal{K}'$.

Key generation algorithm $\mathcal{G} : H_B \to \mathcal{K} \times \mathcal{K}'$.

$\mathcal{G}$ is a probabilistic algorithm that outputs a key pair $(K, K') \in \mathcal{K} \times \mathcal{K}'$ chosen according to the channel H_B between the transmitter and the receiver.

Encryption algorithm $\mathcal{T} : M \times \mathcal{K} \to \mathcal{C}$.

Channel function $H_B : \mathcal{C} \to \mathcal{Z}$ and $H_E : \mathcal{C} \to \mathcal{Z}$

$\mathcal{H}$ is the equivalent channel function between cipher signal Y and received symbol Z_B, $Z_B = H_B(Y)$. $\mathcal{Z}$ is the set of all possible Z_B, and $Z_B \in \mathcal{Z}$. H_E is the channel function of eavesdropper.

PRCNG: $\mathcal{P} : \mathcal{K} \to \mathbb{C}^n$.

$\mathcal{K}$ is the key set and $\mathbb{C}^n$ is a $(n \times 1)$ complex vector space; for stream PLE, complex sequence $\{r_n\} = \{r_1, r_2, \ldots\} \in \mathbb{C}^n$.

Decryption algorithm $\mathcal{D} : \mathcal{Z} \times \mathcal{K}' \to \mathcal{M}$.

From the above definition we can see two characteristics of PLE different from traditional encryption:

1. The cipher signal space is different. The cryptographic signal space in the PLE is a complex field, which requires us to design the PLE function of the complex field.

2. The input signal of the decryption algorithm is different. In the PLE system, the signal received by the receiver is affected by noise and channel fading. So the receiving algorithm is a joint detection and decryption algorithm. The decoding algorithm needs to meet the following conditions:

$$\Pr(\mathcal{D}(H_B(T_K(S))) = S) \geq 1 - \delta_e \tag{8}$$

where δ_e is a given error threshold.

Finally, the PLE system cryptographic primitives are expressed as follows:

Block PLE: $\prod_B = (\mathcal{G}, \mathcal{T}, \mathcal{D}, H_B, H_E)$,

Stream PLE: $\prod_S = (\mathcal{G}, \mathcal{T}, \mathcal{D}, H_B, H_E, \mathcal{P})$.

F. SECURITY DEFINITION

Evaluating the ''security'' of an encryption scheme is a very tricky business. The first task is to understand what ''security'' is. There are two types of security. The first one is Shannon's definition of perfect security which requires that the ciphertext contains no information regarding the plaintext. The second one is semantic security which is based on computational-complexity. An encryption scheme is semantically secure if it is *infeasible* to learn anything about the plaintext from the ciphertext. Infeasible means that Eve cannot crack within a given computing complexity.

Here we give the definition of semantic security for PLE.

Definition 3 (Indistinguishability of Encryptions): An PLE scheme $\prod = (\mathcal{G}, \mathcal{T}, \mathcal{D}, H_B, H_E)$ is (t, ϵ) message indistinguishable, if for every two messages S, S', and for every binary output function D_E of complexity $\leq t$, we have

$$|\Pr[D_E(H_E(T_K(S))) = 1] - \Pr[D_E(H_E(T_K(S'))) = 1]| \leq \epsilon, \tag{9}$$

where the probability is taken over the randomness of $T_K(S)$, the choice of $K \in \mathcal{K}$ and the channel H_E. (Typical parameters that are considered in practice are $t = 2^{80}$ and $\epsilon = 2^{-60}$.)

In realistic scenarios, Eve may have knowledge of plaintext-ciphertext pairs. If Eve is able to see encryptions of arbitrary messages of her choice, she may get some information of key or plaintext. An attack in this model is called a CPA. Now, we will give a security definition under CPA for PLE.

Definition 4 (Message Indistinguishability Against CPA): An PLE scheme $\prod = (\mathcal{G}, \mathcal{T}, \mathcal{D}, H_B, H_E)$ is (t, ϵ)-message indistinguishable against CPA if for every two messages S, S' and every D_E of complexity $\leq t$ we have

$$|\Pr[D_E^{H_E(T_K(S))}(H_E(T_K(S))) = 1] - \Pr[D_E^{H_E(T_K(S))}(H_E(T_K(S'))) = 1]| \leq \epsilon \tag{10}$$

where $D_E^{H_E(T_K(.))}(H_E(T_K(S)))$ means the computation of algorithm D_E given $H_E(T_K(S))$ as an input and given the ability to execute $H_E(T_K(.))$.

In (9) and (10) H_E is a random function that makes the result of each encryption different even if the plaintext is the same. This is because the channel is random and we also can add artificial noise at the transmitter.

III. THE DESIGN FRAMEWORK AND RULES OF PLE

In this section, we will study the design rules and framework of PLE. There are two aspects to consider when designing the PLE algorithms.

(i) *Reliability*

We need to make sure that the legitimate receiver can recover the received signal correctly and easily. When designing encryption and decryption algorithms, the effects of noise and channel need to be taken into account. We need to ensure the maximum constellation distance for better BER performance. We also need to consider reducing the complexity of the receiver.

(ii) *Security*

The PLE constellation should be diffusing and confusing. We should effectively use the influence of channel and noise to increase the difficulty of cracking. The designed PLE algorithm should be able to resist brute force attacks and various types of attacks.

In the design of the PLE, reliability and security need to be considered together. The encryption and decryption algorithms used in the PLE should not sacrifice bit error rate performance. The stream PLE and block PLE structures are quite different, so we will discuss them separately as follows.

A. STREAM PLE DESIGN FRAMEWORK

As shown in Fig.3, the design of the Stream PLE module consists of two parts. The first part is to design the PRCNG module. According to Definition 1, we need to generate a pseudo-random complex sequence that obeys a particular distribution. This pseudo-random complex sequence is a deterministic algorithm, and Alice and Bob generate the same

pseudo-random complex sequence from a short true random seed (Key). Pseudo-random number generation algorithms have been studied in many works such as [25].

The second part is the encryption function f in (2). In stream PLE, the encryption function f maps the input information bits into a complex signal (constellation point) according to the pseudo-random complex sequence r_n. We need to consider the design of f from both a reliability and security perspective. Therefore, we use the following two indicators as the optimization goals of the design f function.

1) MINIMUM CONSTELLATION DISTANCE

$$d = \min_{(i,j)i\neq j} \left| f(s_i, r_n) - f(s_j, r_n) \right| \tag{11}$$

where s_i, $s_j \in \mathcal{M}$ are possible input messages and d is the minimum distance between two different constellations. Like the traditional constellation design, d determines the error probability at the receiver. So our design goal is to maximize d to minimize BER.

2) CONFUSION CHARACTERISTICS OF THE OUTPUT SIGNAL

Note that if r_n is truly random, then this forms a one-time system which provides perfect security. However, in a practical system, we cannot get a truly random r_n from a limited length key. So r_n is a pseudorandom complex sequence and not truly random. Therefore, eavesdroppers have the possibility of obtaining information about s_i or r_n by accumulating observations for Y over a long time. In order to avoid this situation, we need more confusion in the y-sequence, and there are more possible values for $y = a + jb$.

We use the continuous entropy to measure the confusion degree of Y as follows:

$$H(Y) = -\int_{-\infty}^{\infty}\int p(a,b)\log_2 p(a,b)dadb, \tag{12}$$

where $p(a, b)$ is the joint probability density function for a and b.

Since continuous entropy is infinite, it is not easy to calculate the continuous entropy values. In addition, the actual digital system will quantize the signal Y, so we will use discrete source entropy to measure the confusion degree of Y. A continuous Y is discretized into bins of size Δ (we can understand it as quantization accuracy). We thus have quantized entropy as:

$$H^{\Delta}(Y) := -\sum_{i=-\infty}^{\infty}\sum_{j=-\infty}^{\infty} \Gamma(i,j)\log_2 \Gamma(i,j), \tag{13}$$

where $\Gamma(i,j) = \int_{i\Delta}^{(i+1)\Delta}\int_{j\Delta}^{(j+1)\Delta} p(a,b)dadb$.

We need to maximize $H^{\Delta}(Y)$, given the domain of Y is $\mathcal{C}$. According to maximum entropy theory, Y needs to be a uniform distribution within its given domain $\mathcal{C}$ [26]. This rule means that for an arbitrary input symbol S, after the f-function transformation, Y can be any value in the entire given domain, and the probability of different values is equal.

According to the above two criteria, we present two design routes for encryption functions.

(i) *PLE based on traditional modulation*

The first design idea is implemented by transforming on the traditional constellation (BPSK,QAM, etc.). We just need to design the transform function for encryption and decryption. The transform function needs to confuse the constellation as much as possible. In addition, in order not to change the BER performance of the original constellation, we need to ensure that the transformation function does not change the distance of the constellation points.

In a phase modulation system (QPSK, BPSK, M-PSK, etc.), a straightforward method is constellation rotation. A random complex signal $e^{-j\theta_n}$ ($\theta \sim U[0, 2\pi]$, uniform distribution) is generated by the PRCSG module, and then multiplied by the original constellation to obtain an encrypted constellation. The encryption process is as follows:

$$Y_n = X_n e^{-j\theta_n}. \tag{14}$$

Obviously, the transformation in (14) does not change the constellation distance. This method is used in [27] and [14]. In [27], three candidate PLE methods based on traditional modulation are proposed and compared. The phase rotation method depends on the phase information shared by both Alice and Bob. The phase information can be extracted from the reciprocal channel or transmitted by a secure channel. The eavesdropper does not know this phase information.

In the amplitude and phase modulation system (e.g.,QAM), both the phase and amplitude information needs to be protected. Only phase rotation will leak the amplitude information. Therefore, we propose a disturbance-rotation method as follows.

First, the input symbol s_n is scrambled to obtain s'_n. This scramble operator destroys the correspondence relationship between the amplitude information and the number of bits.

Take 16QAM as an example, the information symbol is $s_n = \{b_1b_2b_3b_4\}$. First, we change the order of the bits according to the pseudorandom number given by the random generator, and get $s'_n = \{b_{a_1}b_{a_2}b_{a_3}b_{a_4}\}$, where $\{a_1, a_2, a_3, a_4\}$ is a permutation of $\{1, 2, 3, 4\}$. Here there are 4! = 24 kinds of possible permutations. Then, we perform 16QAM mapping to get X_n. Finally we use the rotation operation as (14) The final constellation is now shown in Fig.4.

(ii) *New constellation for stream PLE*

Another effective method is to design a new PLE constellation. This makes the constellation diagram have better confusing characteristics, which can resist brute force cracking.

For example, a 3-dimensional rotated constellation modulation was proposed in our previous work [28]. We map each 2-bits message to a 3-dimensional constellation point and evenly distributed on the spherical surface. The 3-dimensional constellation points occupy 3 real channels in the practical system. For example, in an OFDM system, we combine 1.5 subcarriers as one modulation unit for three-dimensional mapping. The detailed process is as follows:

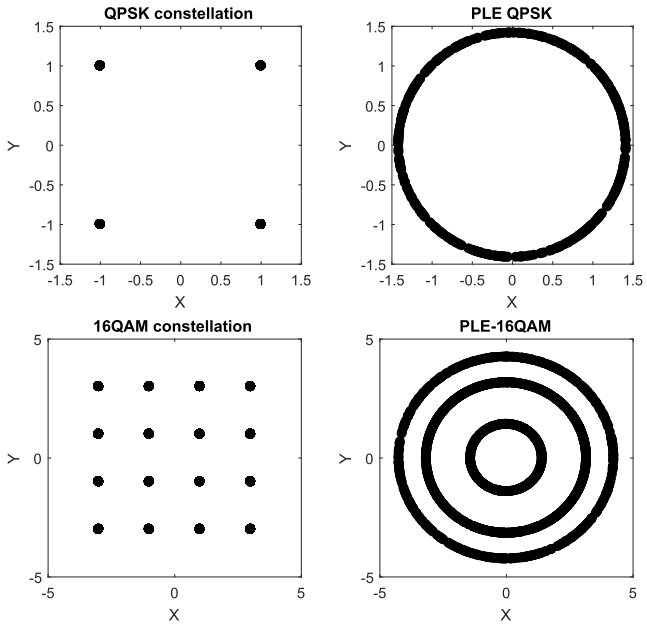

FIGURE 4. PLE for QPSK and 16QAM systems.

First, we map each 2-bit message s_n into the vertex coordinates of a regular tetrahedron $\{V_1, V_2, V_3, V_4\}$ according to equation (15), as shown in Fig. 5, where $X_n \in \mathbb{R}^3$.

$$X_n = \begin{cases} V_1 & \text{if } s_n = 00 \\ V_2 & \text{if } s_n = 01 \\ V_3 & \text{if } s_n = 11 \\ V_4 & \text{if } s_n = 10. \end{cases} \tag{15}$$

The regular tetrahedron constellation has better energy efficiency.

An example of appropriate vertices are:

$$\begin{aligned} V_1 &= (\sqrt{8/9}, 0, -1/3) \\ V_2 &= (-\sqrt{2/9}, \sqrt{2/3}, -1/3) \\ V_3 &= (-\sqrt{2/9}, -\sqrt{2/3}, -1/3) \\ V_4 &= (0, 0, 1) \end{aligned} \tag{16}$$

Next, we use three-dimensional rotation to disturb the constellation for security.

$$Y_n = R(\alpha, \beta, \gamma) \cdot X_n \tag{17}$$

where $Y_n \in \mathbb{R}^3$, $R(\alpha, \beta, \gamma) \in \mathbb{R}^{3\times3}$ is the rotation matrix and $\alpha, \beta, \gamma \sim U(0, 2\pi)$ are phase parameters. $R(\alpha, \beta, \gamma)$ is given by (18) and (19), as shown at the bottom of the next page.

The distribution of Y_n is shown in the Fig.5. These constellation points (Y_n) are distributed on the surface of the unit sphere with centroid at the origin.

B. BLOCK PLE DESIGN FRAMEWORK

The operating unit of the Block PLE is a fixed-length binary sequence. Unlike the traditional block cipher, block PLE converts bit blocks to complex vectors. The rules of Block

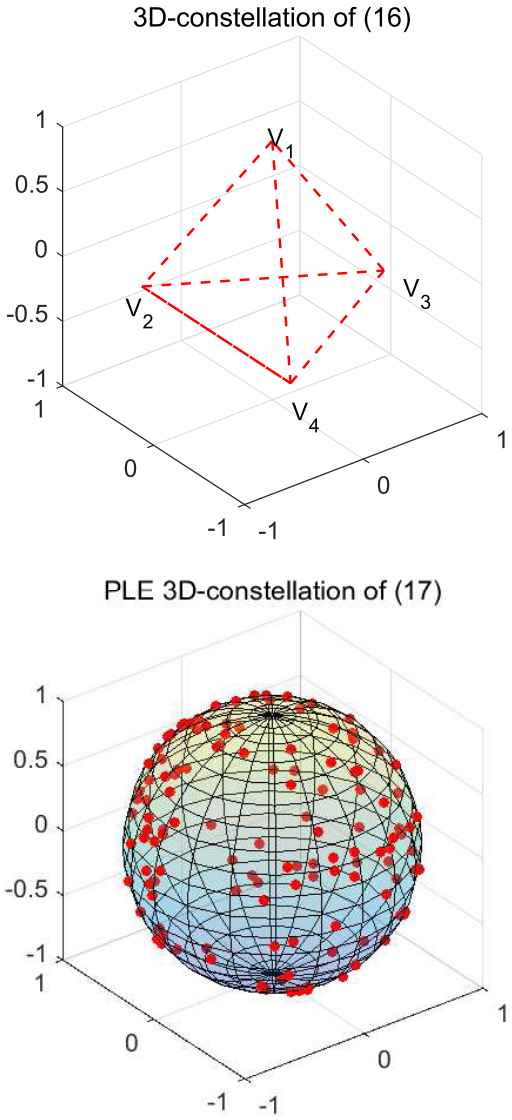

FIGURE 5. PLE for a 3-D constellation where constellation points lie on the surface of the sphere with a uniform probability density function for each of the two parametric angles.

PLE is different from upper layer block cipher. Traditional Block cipher is faced with an ideal noise-free channel (as show in Fig. 1, the error has been removed by the channel coding and modulate module). The Block PLE is faced with a channel with noise and channel fading as show in Fig. 2. It is designed not only to take into account the security but also to take into account the reliability. So the Block PLE design is a joint design of communication and encryption.

The design of block PLE needs to consider the following three aspects.

(i) *Confusion*

The relationship between the key and the cipher signal is very complicated and there is no clear correspondence. A small change in the key will make the cipher signal completely different. Even if the eavesdropper has a large amount of cipher signal, the key cannot be analyzed.

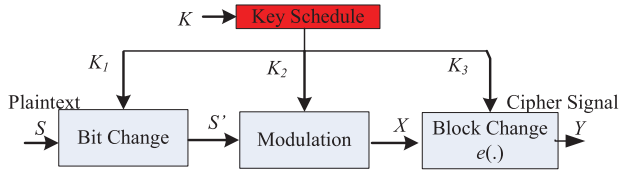

FIGURE 6. Block PLE.

(ii) *Diffusion*

We should make the statistical structure of the plaintext dissipate over the entire cryptographic signal. The correspondence between plaintext and cipher signals should be disturbed and complicated as much as possible. The diffusion feature is designed to prevent differential attacks. Note that this is a little different from the diffusion concept in traditional bit-level encryption. In traditional bit-level encryption, changing one bit of plaintext will make the cipher text totally different. However in PLE, due to channel noise, we should ensure that the distances between the plaintext codes do not change after encryption to guarantee the bit error rate of the legal receiver.

(iii) *Noise tolerance*

Since the cipher signal passes through the wireless channel. The receiver needs to recover the message from the cipher signal containing noise. Therefore, the design of the encryption and decryption functions should not amplify the noise.

Fig. 6 is the structure of block PLE. The key schedule is an algorithm that extends a short master key K to three different extended keys (K_1, K_2, K_3) for the following three PLE stages [29]. The three stages are: Bit Change, Modulation and Block Change.

The purpose of the bit change stage is to disturb and confuse binary sequences. We can use Boolean operations such as interleaving, replacement,permutation, etc. [30], [31]. The binary vector $\mathbf{S}$ is changed to $\mathbf{S}'$ according to K_1.

The modulation stage maps binary sequences to complex vectors:

$$\mathbf{S}' = \{s'_1 s'_2 \dots s'_l\} \rightarrow \mathbf{X} = \{X_1 X_2 \dots X_N\},$$

where $\{s'_1 s'_2 \dots s'_l\}$ are binary numbers, and $\mathbf{X} \in \mathbb{C}^N$ is the output of the modulation. l is the bits length and N is the symbol number. For M-ary constellation, $l = N \log_2 M$.

Block change is the most important step in the PLE. Its function is to make the symbols interlace and confuse, so that the eavesdropper can not recover the original signal. Essentially, it is a mapping function e between two complex vector spaces:

$$\mathbf{X} = \{X_1 X_2 \dots X_N\} \rightarrow \mathbf{Y} = \{Y_1 Y_2 \dots Y_N\} \tag{20}$$

$$\mathbf{Y} = e(\mathbf{X}) \tag{21}$$

where $\mathbf{Y} \in \mathbb{C}^N$ is the cipher signal vector. We can design multiple sub-transforms $e_1, e_2, e_3 \dots$ and then combine them to form e.

$$e(\mathbf{X}) = e_1(e_2(\dots(e_n(\mathbf{X})))). \tag{22}$$

We provide three types of transforms for PLE, which are isometry transformation, stochastic transformation and nonlinear transformations.

1) ISOMETRY TRANSFORMATION

In order to make the distance of the constellation points not change, we use the definition of isometry.

Definition 5: Let X and Y be metric spaces with metrics d_X and d_Y: A map $f : X \rightarrow Y$ is called an **isometry** or **distance preserving** if for any $a, b \in X$ one has

$$d_Y(f(a), f(b)) = d_X(a, b). \tag{23}$$

Then X and Y are Euclidean spaces of the same dimension N, and all the isometries between X and Y can be denoted by premultiplying X with a unitary matrix $\mathbf{U} \in \mathbb{C}^N$ where

$$\mathbf{U}\mathbf{U}^{\mathrm{H}} = \mathbf{U}^{\mathrm{H}}\mathbf{U} = \mathbf{I}_N. \tag{24}$$

Obviously $|\det(\mathbf{U})| = 1$. The columns or rows of $\mathbf{U}$ form an orthonormal basis of $\mathbb{C}^N$ with respect to the usual inner product. In fact any $N \times N$ unitary matrix $\mathbf{U}$ has N^2 independent real phase parameters. Thus, we can generate an $N \times N$ unitary matrix $\mathbf{U}$ from a given rotation direction vector, $\Phi \in \mathbb{R}^{N^2}$. Φ can be generated from K_3 (see Fig. 6), and both are known by both Alice and Bob. The method of generation of an $N \times N$ unitary matrix from Φ is given in [32].

Taking $N = 2$ as an example then the general expression for an 2×2 unitary matrix is:

$$\mathbf{U} = e^{i\phi/2} \begin{bmatrix} e^{i\phi_1} \cos\theta & e^{i\phi_2} \sin\theta \\ -e^{-i\phi_2} \sin\theta & e^{-i\phi_1} \cos\theta \end{bmatrix}, \tag{25}$$

which depends on 4 parameters $\Phi = \{\phi, \phi_1, \phi_2, \theta\}$, where $\phi, \phi_1, \phi_2, \theta \in [0, 2\pi]$.

Thus $e_i(\mathbf{X}) = \mathbf{U}\mathbf{X}$ (see (22) for $e_i(\mathbf{X})$) can be used as a sub-transformation. We can also extend to $N > 2$ to acquire more confusion.

Theorem 6: For any M-ary constellation diagram $\mathbf{S} = \{\mathbf{S_1}, \mathbf{S_2}, \dots, \mathbf{S_M}\}$, *an isometry transformation* $e(\dots)$ *on* $\mathbf{S}$

$$R(\alpha, \beta, \gamma) = \begin{bmatrix} \cos\gamma & \sin\gamma & 0 \\ -\sin\gamma & \cos\gamma & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\beta & \sin\beta \\ 0 & -\sin\beta & \cos\beta \end{bmatrix} \begin{bmatrix} \cos\alpha & 0 & \sin\alpha \\ 0 & 1 & 0 \\ -\sin\alpha & 0 & \cos\alpha \end{bmatrix} \tag{18}$$

$$= \begin{bmatrix} \cos\alpha\cos\gamma - \cos\beta\sin\alpha\sin\gamma & \sin\alpha\cos\gamma + \cos\beta\cos\alpha\sin\gamma & \sin\beta\sin\gamma \\ -\cos\alpha\sin\gamma - \cos\beta\sin\alpha\cos\gamma & -\sin\alpha\sin\gamma + \cos\beta\cos\alpha\cos\gamma & \sin\beta\cos\gamma \\ \sin\beta\sin\alpha & -\sin\beta\cos\alpha & \cos\beta \end{bmatrix} \tag{19}$$

does not change its average demodulation BER performance under Additive White Gaussian Noise (AWGN) channels.

Proof: We assume that after isometry transformation, the constellation diagram turns into $\mathbf{Y} = \{Y_1, Y_2, \ldots, Y_M\}$. According to Definition 1, for any $i, j \leq M$, we have

$$\left\|\mathbf{S_i} - \mathbf{S_j}\right\| = \left\|\mathbf{Y_i} - \mathbf{Y_j}\right\|.$$

We assume the channel output of the S system and the Y system are $r = \mathbf{S_i} + n_1$ and $\tilde{\boldsymbol{r}} = Y_i + n_2$ respectively, where n_1 and n_2 are i.i.d. Gaussian noise vectors.

The maximum likelihood (ML) receivers of constellation diagram $\mathbf{S}$ and $\mathbf{Y}$ are

$\underset{S_i}{argmin} \|r - \mathbf{S_i}\|$ and $\underset{Y_i}{argmin} \|\tilde{\boldsymbol{r}} - \mathbf{Y_i}\|$.

The $\mathbf{S_i}$ and $\mathbf{Y_i}$ $(i = 1, \ldots sM)$ are determined from the decision regions:

$$Z_i = (r : ||r - \mathbf{S_i}|| < ||r - \mathbf{S_j}||, \forall j = 1, \ldots, M,\ j \neq i) \quad (26)$$

$$\tilde{Z}_i = (\tilde{\boldsymbol{r}} : ||\tilde{\boldsymbol{r}} - \mathbf{Y_i}|| ||\tilde{\boldsymbol{r}} - \mathbf{Y_j}||, \forall j = 1, \ldots, M,\ j \neq i). \quad (27)$$

According to Definition 3, for any r we have

$$\left\|r - \mathbf{S_j}\right\| = \left\|\tilde{\boldsymbol{r}} - \mathbf{Y_j}\right\|, (j = 1, \ldots, M) \quad (28)$$

Thus according to (26), (27) and (28), Z_i and $\tilde{Z}_i$ are in one-to-one correspondence.

The error probability of the ML receiver of constellation diagrams $\mathbf{S}$ and $\mathbf{Y}$ are

$$\begin{aligned} P_e &= \sum_{i=1}^{M} p(r \notin Z_i | S_i \, sent) p(S_i \, sent) \\ &= 1/M \sum_{i=1}^{M} p(r \notin Z_i | S_i sent) \\ &= 1 - 1/M \sum_{i=1}^{M} p(r \in Z_i | S_i sent), \end{aligned} \quad (29)$$

and

$$\tilde{P}_e = 1 - 1/M \sum_{i=1}^{M} p(\tilde{\boldsymbol{r}} \in \tilde{Z}_i | \mathbf{Y_i} sent). \quad (30)$$

Due to Z_i and $\tilde{Z}_i$ being in one-to-one correspondence, $P_e = \tilde{P}_e$, so the two constellation diagrams $\mathbf{S}$ and $\mathbf{Y}$ have the same demodulation performance. ■

Although the above proof assumes an AWGN channel, the simulations section shows that the conclusions are also correct under multipath fading channels.

The phase rotation scheme, which has been used in [12], [14], [17], [33], is a specific example of isometry — i.e., diagonal matrix:

$$\mathbf{U} = \begin{bmatrix} e^{i\phi_1} & & & \\ & e^{i\phi_2} & & \\ & & \ddots & \\ & & & e^{i\phi_N} \end{bmatrix} \quad (31)$$

where $\phi_1 \phi_2 \ldots \phi_N \in [0, 2\pi]$ are taken as keys. Multiplying a vector by this matrix means that each element of the vector rotates at different angles $\phi_1 \phi_2 \ldots \phi_N \in [0, 2\pi]$.

However, it is not safe to use only phase rotation, which cannot resist known-plaintext attacks. We will analyze this issue in the section IV.C.2.

2) STOCHASTIC TRANSFORMATION

If the eavesdropper can obtain a large number of plaintext cipher signal pairs, then it can perform known-plaintext attacks or statistical analysis attacks. To combat these attacks, we should introduce a random transformation. The stochastic transformation makes the cipher signal different even if the plaintext is the same. A simple example of stochastic mapping is to add some restricted artificial noise.

3) NONLINEAR TRANSFORMATIONS

Ordinary non-linear transformations will amplify the effects of noise. So squared functions and exponential functions cannot be applied directly to PLE systems. However, we can consider a system under low noise, and using some special non-linear transformations we will have a more secure effect.

The purpose of these transformations is to make each input bit dispersed into the entire output signal block, and to make the output signal confusing, while ensuring that the BER performance of the system does not decrease. Similar to stream PLE, we can still use the quantized information entropy of the constellation as in (13) to measure the degree of confusion in the overall Block PLE system.

C. BLOCK PLE MODE OF PRACTICAL OPERATION

Block PLE by itself is only suitable for the secure transformation of one fixed-length group of bits called a block. In order to securely transform amounts of data larger than a block, we also need to design the mode of operation for block PLE. A mode of operation describes how to repeatedly apply a block PLE single-block operation. In this section we will introduce a natural and simple operation mode called Electronic Codebook (ECB). We then propose a new operation mode PLE-block chaining (PBC).

1) ELECTRONIC CODEBOOK (ECB)

A simple encryption mode is the Electronic Codebook (ECB) mode as shown in Fig.7. The messages that need to be encrypted are divided into blocks according to the block size of the block cipher, and each block is independently encrypted. The disadvantage of this method is that the same plaintext block is encrypted into the same cipher signal block. Therefore, it does not hide data patterns well and can be easily cryptanalyzed.

2) PLE-BLOCK CHAINING (PBC)

Inspired by the Cipher-block chaining(CBC) model [34], we proposed the PLE-block chaining mode. In PBC mode, as shown in Fig.8 each plaintext block is XORed with the bit change output S' from the previous PLE block and then

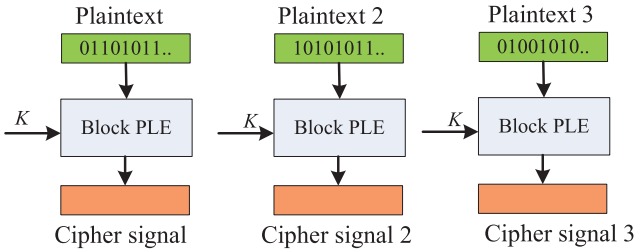

FIGURE 7. Electronic Codebook (ECB).

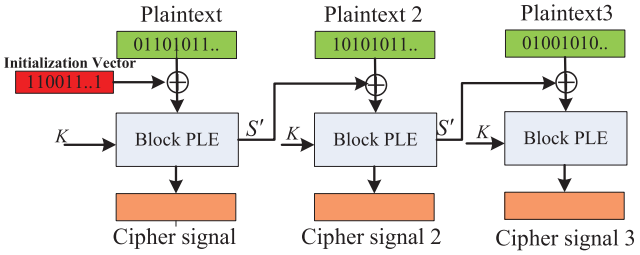

FIGURE 8. PLE-block chaining (PBC).

encrypted by PLE. In this method, each cipher signal block depends on all plaintext blocks in front of it. At the same time, in order to ensure the uniqueness of each message, you need to use the initialization vector in the first block.

D. DESIGN PRINCIPLES FOR IMPLEMENTATION PLE

A good PLE should be hard to break and easy to implement. Both the encryption function and the decoding function should be easily computable. PLE is usually implemented in hardware, such as a VLSI-chip. To reduce complexity and make it easier to standardize, the following design principles are required:

1) **Independence and universality:** Design PLE as a separate module embedded in the communication system that can be applied to various types of communication systems and modulation types.
2) **Robustness and effectiveness:** The performance of the communication system should not be reduced by PLE, including synchronization performance, channel estimation performance, spectrum efficiency, energy efficiency, etc. And low latency is also important.
3) **Protection of the communications system:** In addition to protecting data, PLEs can also be designed to protect training symbols so that eavesdroppers cannot perform channel estimation and synchronization, thereby achieving stronger security effects.

IV. SECURITY ANALYSIS AND DISCUSSION

In this section we will discuss the security of the PLE system. We also use Kerckhoff's assumption: the enemy knows all details of the system except for the value of the secret key.

A. EAVESDROPPER MODEL

Assume that Eve has the following capabilities:

- Eve can accurately estimate the channel functions $H_B(.)$ and $H_E(.)$.
- Eve knows the encryption function f and decryption function D, but does not know the secret key K.

Eve may use the following attack methods:

- Eve only knows Z_E^n and try to decode S or recover K (ciphertext-only attack).
- Eve knows the plaintext S and its corresponding ciphertext signal Z_E^n, and attempts to recover K (known-plaintext attack).
- Eve can obtain the cipher signal for any specified plaintexts for the current key, and attempts to recover K (chosen-plaintext attack).

The PLE algorithm we designed needs to be able to resist the above attacks. From equation (7), we can see that even with the same transmission symbol S and the same key K, due to noise and influence of the channel, at different transmission timings the results Z_E obtained will be different. S and Z_E does not show a one-to-one correspondence, which makes eavesdropper cryptanalysis methods such as linear attacks and differential analysis more difficult.

B. STREAM PLE SECURITY DISCUSSION

First, we analyze the signals received by eavesdropper,

$$Z_E^n = H_E(y_n) = H_E(f(s_n, r_n)).$$

The security of the stream PLE system is mainly guaranteed by the pseudorandom complex sequence r_n and the encryption function f. Therefore, the security features that need to be considered during design are as follows:

1. We need the autocorrelation function of r_n to have a distinct peak, and the period of the r_n sequence should be longer than the lifetime of the key.

2. The design of the function $y_n = f(s_n, r_n)$ should make the output signal y_n uniformly and randomly distributed. Its distribution characteristics are not affected by the input signal s_n, and the eavesdropper cannot perform statistical analysis from the received signals.

Shannon proved in theory that the one-time pad cipher is perfectly secure in the ciphertext-only scenario. But how to generate the pseudorandom complex sequence r_n which is close to the completely random sequences becomes the key point.

In the stream PLE, the PRCS and the plaintext message are independent of each other. The internal state of the stream is only dependent on the internal state of the last time interval and is not related to the input plaintext. The advantage of the synchronization stream PLE is its limited error propagation. When the transmission error occurs in a symbol, it does not affect the subsequent symbol.

For the known plaintext attack, the attacker can only calculate the pseudorandom complex number r_i at the current time. This is because there is no periodicity or the periodicity is longer than the key lifetime, and there is no correlation with other time intervals. So eavesdroppers cannot get keys

or other plaintext. A well-designed stream PLE can withstand known plaintext attacks.

C. BLOCK PLE SECURITY DISCUSSION

1) KEY SPACE

Security in block PLE is mainly provided by Bit change and Block change. We assume a PLE scheme that maps l bit data into N constellation symbols as in (5). For a block PLE to be secure, its block length l and key size k_l must both be large enough to deter statistical analysis and make the exhaustive key search attack infeasible. In order to facilitate the communication system, N can often be designed as a physical layer signal unit such as the frame length. Since the cipher signal space $\mathbb{C}^N$ is a complex space with infinite values, the available key space is almost infinite. In a practical system, we can choose the corresponding key length according to our needs.

Taking the IEEE 802.16 standard OFDM signal as an example, in a 256-point FFT system, 192 subcarriers carry signals and QPSK modulation is used. Thus, $l = 384$, $N = 192$, and so we can set the key length to 256. Then the key space is 2^{256}. So, brute-force attack is practically impossible for block PLE.

2) KNOWN PLAINTEXT ATTACK AND CHOSEN-PLAINTEXT ATTACK

In order to combat KPA and CPA, we need to design the encryption function $e(x)$ which make Eve cannot recover K from the accumulated large number of plaintext-cipher signal pairs. We consider the worst case that the noise received by Eve is very small and can be ignored. Thus, We assume that Eve can get $\mathbf{Y}$ accurately.

In the phase rotation method [14], [17], [19], each symbol is encrypted separately, $U_n, X_n, Y_n \in \mathbb{C}$. Thus, we have

$$Y_n = e(X_n) = U_n X_n.$$

If the eavesdropper knows X_n and Y_n, it can solve $U_n = Y_n/X_n$ and calculate the key K from U_n. So just using phase rotation is not enough to resist KPA and CPA.

In our proposed Block PLE frame, the signal is encrypted as a group. The unitary matrix $\mathbf{U}$ defined in the isometry transformation has $N \times N$ matrix elements, so Eve cannot solve equation $\mathbf{Y}_{N\times 1} = \mathbf{U}_{N\times N}\mathbf{X}_{N\times 1}$ to obtain $\mathbf{U}$. Moreover, $\mathbf{U}$ will change between different symbols which is guaranteed by *PLE-block chaining (PBC)* as is shown in Fig.8. Thus, Eve cannot obtain $\mathbf{U}$ by accumulating a certain amount of both $\mathbf{Y}$ and $\mathbf{X}$.

V. PERFORMANCE COMPARISON AND NUMERICAL SIMULATIONS

A. PERFORMANCE COMPARISON OF DIFFERENT PLE SCHEMES

To compare the performance of PLE, we considered five PLE algorithms: phase rotation scheme [14], [17], [19], intrinsic interference scheme [12], sub-carrier obfuscate and dummy [11], the proposed isometry based block PLE scheme, and the proposed stream PLE framework. We evaluate algorithm performance from five perspectives: a) BER penalty, reduced BER performance compared to unencrypted systems; b) throughput decrease; c) key space; d) CPA security, the ability to prevent CPA; e) encryption and decryption complexity.

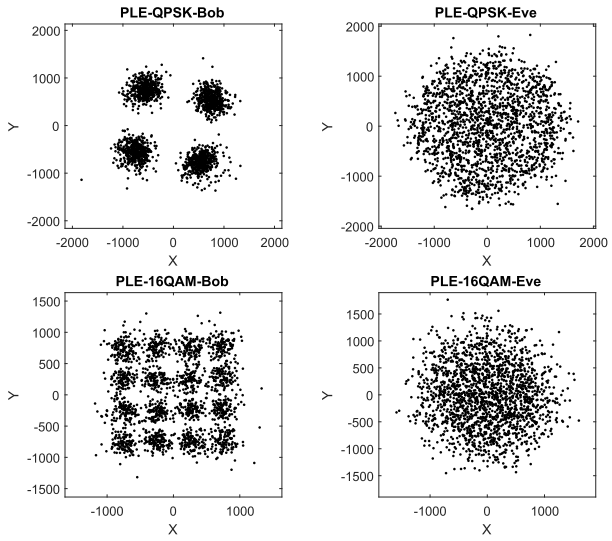

FIGURE 9. The constellation received by Bob and Eve, QPSK and 16QAM, isometry based block PLE OFDM system, SNR=16dB, SUI 1 channel [35].

As shown in Table 2, the proposed PLE methods has advantages over other PLE methods. In the previous section we proved that PLE methods that only uses phase rotation cannot fight CPA. The intrinsic interference scheme and the dummy based scheme use some transmission power to send imaginary symbols or dummy data, so their BER or throughput performances decrease. Note that in the subcarrier obfuscate and dummy scheme two stream ciphers are used, so the CPA security depends on the stream cipher it chooses. Also, the CPA security of the stream PLE framework depends on PRCNG.

We also consider complexity of all the schemes. In the isometry based block PLE scheme, the main added computational complexity is $N \times N$ complex matrix multiplication which is has mature method for hardware implementation. Here, n is the plaintext length. It is shown that all five PLE schemes have linear complexity that can be realized by software or hardware implementation.

B. NUMERICAL SIMULATIONS ON A PRACTICAL OFDM SYSTEM

The performance of the proposed isometry based block PLE scheme is evaluated through numerical simulations. The simulation is based on the physical layer of IEEE 802.11ac OFDM protocol which has been widely used in a wireless local area network. We consider the 256-point FFT with a cyclic prefix length of 1/4 of FFT length. The parameters are: QPSK and 16QAM modulation, DFT size = 256, a cyclic

TABLE 2. Performance comparison of different PLE schemes.

	BER penalty	Throughput decrease	Key space	CPA security	Complexity
Phase rotation scheme [14], [17], [19]	No	No	High	No	$O(n)$
Intrinsic interference scheme [12]	1dB-4dB	No	High	No	$O(n)$
Subcarrier obfuscate and dummy [11]	No	$\alpha = k/(N_d s)$ *	High	Relies on stream cipher	$MO(n)$
Proposed isometry based block PLE	No	No	High	Good	$O(n)$
Proposed stream PLE framework	No	No	High	Relies on PRCNG	$O(n)$

* s is OFDM symbol number in one group, k is the reserved subcarrier number for dummy data, N_d is the subcarrier number, and n is the plaintext length.

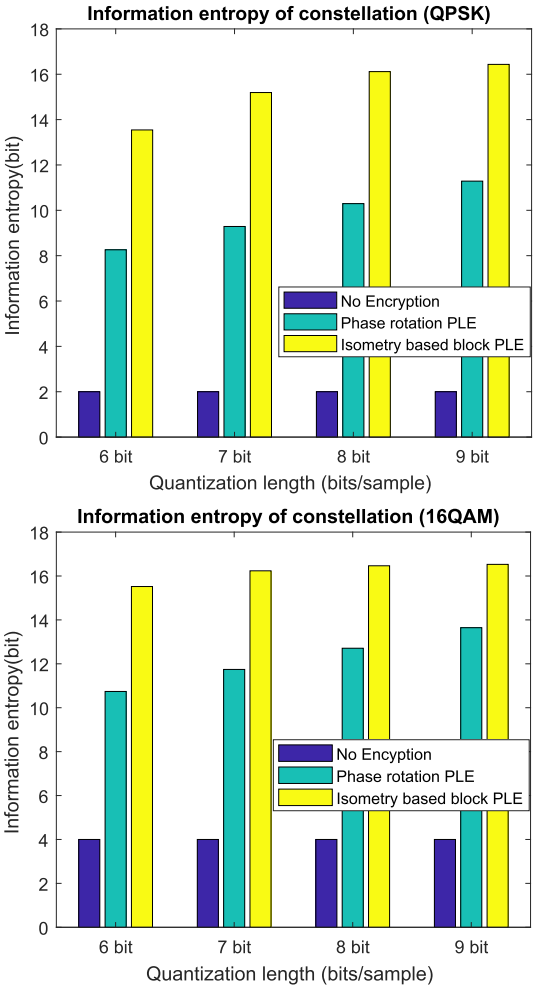

FIGURE 10. Information entropy of constellation.

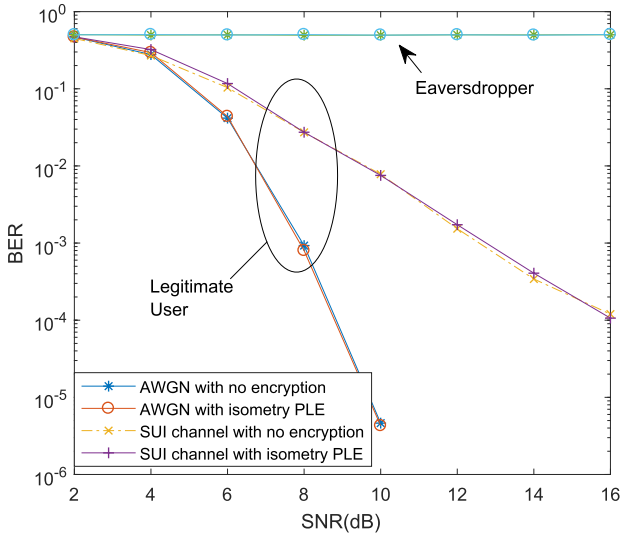

FIGURE 11. BERs of the legitimate user and the eavesdropper in an OFDM system.

prefix length = 64. We evaluate the BER performance over practical frequency selective fading channel SUI models [35].

Fig.9 shows the constellation received by Bob (after decryption recovery) and Eve. As an example, we consider QPSK and 16QAM modulation, the proposed isometry based block PLE OFDM system, SNR = 16 dB. We can see that the constellation symbols received by Eve are approximately uniformly distributed randomly within the given domain under the effects of isometry transformation, while Bob can recover the constellation correctly. Note that in a 16QAM modulation system, the amplitude information is protected in our proposed method. However, the phase rotation scheme in [14], [17], [19] leaks the amplitude information in the 16QAM system as shown in Fig.4.

In order to measure the information leak and confusion degree of constellations, we calculate the information entropy of constellations according to (13). The bigger the entropy is, the more uncertainty the constellation information is, and the less leak information the constellation has. We consider different quantization length (i.e. bits/sample). Fig.10 shows that the information entropy increases with increasing quantization length of constellation coordinates. It is shown that our proposed isometry based method outperforms other methods, and can resist the attacks based on the information entropy.

Then, we evaluate the BERs of the legitimate user and the eavesdropper under an AWGN channel and a SUI channel. In Fig.11, we considered four situations: AWGN channel with no encryption, AWGN channel with PLE, SUI channel with no encryption, and SUI channel with PLE. We can see that in PLE system the eavesdropper's BERs are very close to 0.5. It means that no information is leaked. Simulation also shows that our proposed isometry method nearly has the same BER as the non-encrypted system under both an AWGN channel and a fading channel. These simulation results are consistent with the Theorem 2 in section III.B which means that the isometry transformation does not affect the BER performance.

VI. CONCLUSIONS

This paper proposed a general mathematical model and cryptography primitive of PLE. Different from traditional

cryptography, PLE is essentially a function design from a binary bit domain to a complex domain. Most of its operations are performed in the complex domain. We defined semantic security for PLE. PLE is divided into two categories: stream PLE and block PLE. The design frameworks and guidelines for stream PLE and block PLE are proposed. For block PLE, we proposed three types of sub-transforms: isometry transformation, stochastic transformation and nonlinear transformation. We further proposed a new mode PLE-block chaining to resist CPA and KPA. Compared with traditional cryptography, PLE is still a new field to be explored and studied, which has more cryptographic signal space and key space. Our proposed PLE framework provides more freedom of design and is resistant to KPA and CPA. Simulation shows that the proposed isometry transformation method has good performances in terms of BER penalty and confusion degree.

In future research, we will consider the impact of the error correction mechanism such as ARQ and FEC on the PLE. In addition, non-linear transformations provide better security to confront cryptanalysis. Whether or not there are non-linear transformations that guarantee the performance of the constellation is also a problem. Asymmetric PLE which does not need to perform key distribution on a private channel can also be cast into a similar framework. The detailed investigation of such framework is beyond the scope of this article and is deferred for the future study.

ACKNOWLEDGEMENT

The authors would like to thank Dr. Junqing Zhang and Dr. Ying Huang for improving the quality of the paper.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[4] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Commun.*, vol. 8, no. 8, pp. 1248–1257, May 2014.
[5] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO frequency selective channels by beamforming and noise generation," in *Proc. 19th Eur. Signal Process. Conf.*, Aug. 2011, pp. 829–833.
[6] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.
[7] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
[8] W. Li, Y. Tang, M. Ghogho, J. Wei, and C. Xiong, "Secure communications via sending artificial noise by both transmitter and receiver: Optimum power allocation to minimise the insecure region," *IET Commun.*, vol. 8, no. 16, pp. 2858–2862, Nov. 2014.
[9] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.
[10] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.
[11] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM physical layer encryption scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2114–2127, Mar. 2017.
[12] M. Sakai, H. Lin, and K. Yamashita, "Intrinsic interference based physical layer encryption for OFDM/OQAM," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1059–1062, May 2017.
[13] T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive mimo," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 5419–5436, May 2017.
[14] 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.
[15] 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.
[16] H. Xu and L. Sun, "Encryption over the air: Securing two-way untrusted relaying systems through constellation overlapping," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8268–8282, Dec. 2018.
[17] A. K. Nain, J. Bandaru, M. A. Zubair, and R. Pachamuthu, "A secure phase-encrypted IEEE 802.15.4 transceiver design," *IEEE Trans. Comput.*, vol. 66, no. 8, pp. 1421–1427, Aug. 2017.
[18] 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.
[19] K. Lai, J. Lei, L. Wen, G. Chen, W. Li, and P. Xiao, "Secure transmission with randomized constellation rotation for downlink sparse code multiple access system," *IEEE Access*, vol. 6, pp. 5049–5063, 2018.
[20] W. Li, D. McLernon, J. Lei, M. Ghogho, S. A. R. Zaidi, and H. Hui, "Mathematical model and framework of physical layer encryption for wireless communications," in *Proc. IEEE Global Commun. (GLOBECOM)*, Dec. 2018, pp. 1–7.
[21] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM Subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.
[22] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: Algorithms and rate optimization," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1831–1846, Aug. 2016.
[23] D. Qin and Z. Ding, "Exploiting multi-antenna non-reciprocal channels for shared secret key generation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2693–2705, Dec. 2016.
[24] 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.
[25] J. E. Gentle, *Random Number Generation and Monte Carlo Methods*. Berlin, Germany: Springer, 2006.
[26] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 1991.
[27] S. Bi, X. Yuan, and Y. J. Zhang. (2012). "Pragmatic physical layer encryption for achieving perfect secrecy." [Online]. Avabilable: https://arxiv.org/abs/1210.5599
[28] X. Li, W. Li, J. Lei, and L. Cheng, "A novel physical layer encryption algorithm based on three dimensional constellation rotation in OFDM system," (in Chinese), *Acta Electronica Sinica*, vol. 45, no. 12, pp. 2873–2880, 2017.
[29] J. Kelsey, B. Schneier, and D. Wagner, "Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and triple-DES," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1996, pp. 237–251.
[30] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Boston MA, USA: Academic, 2009, pp. 157–191.
[31] M. A. Khan, M. Asim, V. Jeoti, and R. S. Manzoor, "On secure OFDM system: Chaos based constellation scrambling," in *Proc. Int. Conf. Intell. Adv. Syst.*, Nov. 2007, pp. 484–488.
[32] D. Mortari, "On the rigid rotation concept in n-dimensional spaces," *J. Astron. Sci.*, vol. 49, no. 3, pp. 401–420, Jul. 2001.
[33] G. S. Kanter, D. Reilly, and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 74–81, Nov. 2009.
[34] W. F. Ehrsam, C. H. W. Meyer, J. L. Smith, and W. L. Tuchman, "Message verification and transmission error detection by block chaining," U.S. Patent 4 074 066 A, Feb. 14, 1978. [Online]. Available: https://patents.google.com/patent/US4074066A/en

[35] V. Erceg, *Channel Models for Fixed Wireless Applications*, IEEE Standard 802.16.3c-01/29rl, 2001. [Online]. Available: https://ci.nii.ac.jp/naid/10021333861/en/

WEI LI received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in communication engineering from the National University of Defence Technology (NUDT), Changsha, China, in 2002, 2006, and 2012, respectively. 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 COMMUNICATIONS LETTERS, in 2014.

DES MCLERNON received the B.Sc. degree in electronic and electrical engineering and the M.Sc. degree in electronics from Queen's University Belfast, U.K., and the Ph.D. degree in signal processing from the Imperial College, University of London. He worked on radar systems research and development at Ferranti Ltd., Edinburgh, U.K. His research interest includes the domain of signal processing for wireless communications. He has published over 320 journal and conference papers in this area. He has supervised over 45 Ph.D. students. His current research interests include PHY layer security, M2M communications, energy harvesting, robotic communications, machine learning for security in SDNs, distributed sensing, stochastic geometry, multi-packet reception, and drone small-cell communications. He was recently runner up in the 2018 Leeds Pub Piano Competition. He is an Associate Editor of the *IET Signal Processing*. Recent conference organization includes the IEEE SPAWC 2010, the European Signal Processing Conference (EUSIPCO) 2013, the IET Conference on Intelligent Signal Processing 2013, 2015, and 2017, London, and the IEEE GLOBECOM 2014, 2015, and 2016 (Workshop on Trusted Communications with Physical Layer Security).

JING LEI received the B.Sc., M.Sc., and Ph.D. degrees from the National University of Defence Technology (NUDT), Changsha, China, in 1990, 1994, and 2009, respectively, where she is currently the Leader of the Communication Coding Group. She was a Visiting Scholar with the School of Electronics and Computer Science, University of Southampton, U.K. She is also a Distinguished Professor with the Department of Communications Engineering, College of Electronic Science, National University of Defence Technology. 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.

MOUNIR GHOGHO received the Ph.D. degree from the National Polytechnic Institute of Toulouse, France, in 1997. He was an EPSRC Research Fellow with the University of Strathclyde, U.K., from 1997 to 2001. In 2001, he joined the University of Leeds, where he was promoted to a Full Professor, in 2008. While still affiliated with the University of Leeds, he joined the Université Internationale de Rabat, in 2010, where he is currently the Director of the ICT Research Laboratory (TICLab) and a Scientific Advisor to the President. He was a member of the IEEE Signal Processing Society SPCOM, SPTM, and the SAM Technical Committee. He is a member of the Steering Committee of the IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING. He was a recipient of the 2013 IBM Faculty Award and the 2000 U.K. Royal Academy of the Engineering Research Fellowship. He chaired many conferences and workshops, including the European Signal Processing Conference (Eusipco) 2013 and the IEEE Workshop on Signal Processing for Advanced Wireless Communications (SPAWC) 2010. He is a EURASIP Liaison in Morocco. He served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING and the IEEE SIGNAL PROCESSING LETTERS. He is an Associate Editor of the *IEEE Signal Processing Magazine*.

SYED ALI RAZA ZAIDI received the Ph.D. degree from the School of Electronic and Electrical Engineering, University of Leeds, Leeds. From 2011 to 2013, he was a Lecturer with the International University of Rabat. From 2013 to 2015, he was with the SPCOM Research Group, U.S. Army Research Laboratory, a funded project in the area of network science. In 2013, he was a Visiting Research Scientist with the Qatar Innovations and Mobility Centre, where he was involved in QNRF-funded project, QSON. He is currently an Assistant Professor in wireless communication and sensing systems with the University of Leeds. He has published over 90 papers in leading IEEE conferences and journals. He is also an active member of the EPSRC Peer Review College. During his Ph.D. degree, he received the G. W. Carter Prize and the F. W. Carter Prize for the best thesis and best research paper, respectively. He is a EURASIP Local Liaison in U.K. and also a General Secretary of the IEEE Technical Subcommittee on Backhaul and Fronthaul networks. From 2014 to 2015, he served as an Editor for the IEEE COMMUNICATION LETTERS. He was a Lead Guest Editor of the *IET Signal Processing*–Special Issue on Signal Processing for Large-Scale 5G Wireless Networks. He is an Associate Technical Editor of the *IEEE Communications Magazine*.

HUAIHAI HUI, photograph and biography not available at the time of publication.