
Proceedings Paper:
Li, W, McLernon, D orcid.org/0000-0002-5163-1975, Lei, J et al. (3 more authors) (2019) Mathematical Model and Framework of Physical Layer Encryption for Wireless Communications. In: Proceedings of 2018 IEEE Globecom Workshops (GC Wkshps). 2018 IEEE Globecom Workshops (GC Wkshps), 09-13 Dec 2018, Abu Dhabi, United Arab Emirates. IEEE . ISBN 978-1-5386-4920-6

https://doi.org/10.1109/GLOCOMW.2018.8644193

Mathematical Model and Framework of Physical Layer Encryption for Wireless Communications

Wei Li[1], Des McLernon[2], Jing Lei[1], Mounir Ghogho[2,3], Syed Ali Raza Zaidi[2] and Huaihai Hui[2]
[1]College of Electronic Science and Engineering, National University of Defense Technology, China. Email: liwei.nudt.cn@gmail.com
[2]University of Leeds, Leeds LS2 9JT, U.K.
Email: d.c.mclernon@leeds.ac.uk, S.A.Zaidi@leeds.ac.uk, huihuaihai@ucas.ac.cn
[3]International University of Rabat, Morocco. Email: m.ghogho@leeds.ac.uk

***Abstract*—As a response to serious transmission security problems in wireless communications, physical layer encryption (PLE) provides an effective security measure which is very different from upper layer cryptography technologies. PLE can take advantage of the effects of channel and noise and the processing objects are complex vector signals, which are essentially different from Boolean algebra based traditional cryptography. This paper establishes mathematical models, design frameworks and cryptographic primitives for PLE. 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. The proposed PLE framework has a large cipher signal space and key space; it provides more freedom in design and can resist known plaintext attacks and chosen-plaintext attacks.**

***Index Terms*—Physical layer encryption, Block PLE, Stream PLE, Isometry transformation, Stochastic transformation, PLE-block chaining**

I. Introduction

With the rapid development of wireless communication technology, transmission security has become a very important issue. Due to the broadcast characteristics of wireless channels, the leakage and decipherment of wireless signal has now become a major security issue. For the confidential communication problem, Shannon's early paper [1] made a seminal contribution, in which confidentiality and reliability are closely combined. However, sophisticated modern cryptography theories recently developed are separated from the foundations of wireless communications. On one hand, modern cryptography considers the problem of encryption via transmission over error-free channels. On the other hand, in communication systems, we consider only the reliability and effectiveness of transmission. In a practical communication system, such as cellular communications or wireless LAN communication, the communication physical layer and the security layer are designed separately and do not have much overlap with each other.

The emergence of physical layer security (PLS) breaks this boundary. Wyner's pioneering work took into account the physical layer security issues in error channels [2]. We call this information theory security. This is a completely different path from traditional cryptography. Following Wyner's work, significant research about PLS has already been carried out, including multi-antenna beamforming [3], artificial noise techniques [4], [5], [6], cooperative interference techniques [7], to name but a few.

Physical layer encryption (PLE) is another approach that is different from PLS. Compared with information theory security, PLE provides a more practical and effective method. The encryption process itself does not rely on channel conditions and it can provide security protection when the eavesdropper's channel is better than the "Alice to Bob" channel. Compared with traditional cryptography (that only considers perfect channels) it can take advantage of the effects of channel and noise and hopefully provide stronger security. The existing literature has adopted PLE methods in OFDM systems [8], [9], massive MIMO systems [10], [11], IEEE 802.15.4 protocols [12] and sparse code multiple access (SCMA) [13]. The work in [12] considers the hardware implementation of the PLE algorithm on ASIC and FPGA designs.

The main methods used in PLE are constellation rotation, sub-carrier disturbance, symbol scrambling, training symbol resequencing and so on. However, many existing PLE methods cannot resist known-plaintext attacks (KPAs) and chosen-plaintext attacks (CPAs). In this paper, we will consider the PLE method which can resist both KPA and CPA.

Furthermore, existing PLE papers lack precise cryptographic primitive definitions and rigorous proofs of security which are very important for building PLE-based practical cryptographic protocols. In this paper, we will concentrate on the general mathematical model and framework of PLE, and propose corresponding standards to measure the security of PLE. One of the main goals of this paper is to establish cryptographic primitives for PLE and summarize the basic design rules.

The main contributions of this paper are:

1) We will divide PLE into *stream PLE* and *block PLE*. We will establish two general-purpose mathematical models and define *cryptographic primitives* for *stream PLE* and *block PLE*.
2) We will propose a *design framework* and the basic rules of both stream and block PLE.
3) We will define the *isometry transformation* and the stochastic transformation in block PLE. We will prove that the proposed PLE frameworks can resist both KPA and CPA.

The remainder of this paper is organized as follows. Section II describes the PLE system model and cryptography primitive.

This work was supported in part by the National Natural Science Foundation of China (Numbers 61502518 and 61702536), Natural Science Foundation of Hunan Province China (No.2018JJ3609) and the China Scholarship Council (CSC) government-sponsored visiting scholar research program.

This work was also partly supported by the UK British Council (Newton Fund) through the Project: "Wireless Sensor Networks for Real Time Monitoring of Water Quality" under Grant IL3264631003.

The design framework and rules of PLE are described in Section III. A security analysis of KPA and CPA is discussed in Section IV. Finally in section V we present some conclusions.

Notation: $\mathbf{X}^T$, $\mathbf{X}^*$, $\mathbf{X}^H$and $\mathbf{X}^{-1}$denote respectively the transpose, conjugate, conjugate transpose and inverse of matrix $\mathbf{X}$. $\mathbf{I}_N$ denotes the N-dimensional identity matrix. $|x|$ denotes the absolute value of a complex scalar x. We will use $\|\cdot\|$ to denote 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 $\mathcal{A}$ and $\mathcal{B}$, $\mathcal{A}\times\mathcal{B} = \{\,(a,b) \mid a \in \mathcal{A} \text{ and } b \in \mathcal{B}\,\}$, where $\times$ is Cartesian product between two sets.

II. PLE System Model and Cryptographic Primitive

A. Comparison between PLE and a traditional cryptography system

A secrecy system is defined as a set of transformations of a message space into a cipher signal space. In traditional cryptography the cipher signal space and the message space are both discrete binary spaces. However, in PLE, the possible cipher signal space is a continuous vector space.

In the traditional security system, it is assumed that the encryption and decryption blocks experience an error-free equivalent channel. We assume that error correction is guaranteed by the channel encoder/decoder module. So modern cryptology has been constructed on the premise of an effectively error free channel. The question is, can we use channel errors to increase the difficulty of deciphering and thus enhance security? PLE will consider this problem and thus combine the encryption and communication modules together.

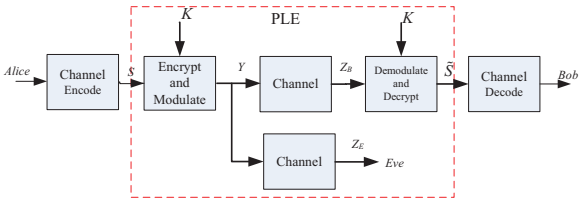

Fig. 1. PLE communication system model.

PLE is a computational, complex-based, security, and its system model is shown in Fig.1. The key still needs to be distributed in the PLE system, which differs from traditional cryptography in that it faces a practical non error-free channel. And its processing object also changes from a binary sequence into a complex sequence. PLE needs to convert the binary sequence S into a complex sequence Y according to the key K, and then it is processed and sent across the channel by the subsequent communication module. In fact, PLE requires the consideration of encryption, but it also needs to consider transmission efficiency and reliability issues. PLE can be thought of as a new extension of cryptography in complex fields and non error-free channels. Since the processing objects are completely different from cryptography, we need to propose new rules and we will also face new problems.

We will now provide a mathematical model and framework of PLE, and we will divide PLE into stream PLE and block PLE.

B. Stream PLE

Stream PLE takes a transmission symbol as a basic processing unit and is a time-varying encryption transform. It has the advantages of fast conversion speed and low error propagation. The hardware implementation circuit is simpler; the disadvantages are: low diffusion and insensitivity to inserts and modifications. The basic model of stream PLE is shown in Fig 2.

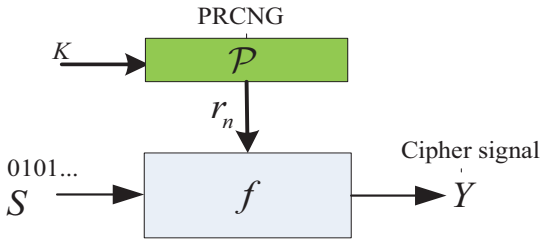

Fig. 2. Stream PLE.

1) Transmitter and channel: First, a series of pseudo-random complex sequences r_n are generated from the initial key *K*:

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

Here, $\mathcal{P}$ is defined as a pseudo-random complex generation function. The distribution of r_n (where n is the symbol index) needs to be designed by the user. It can be fixed in amplitude, uniform in phase distribution, or evenly distributed in real and imaginary parts. For simplification, *n* will later be omitted.

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 $\forall K \in \mathcal{K}$, $\mathcal{P}(K) = \{r_1, r_2, r_3 ...\}$, where $\{r_n\}$ is a sequence of complex independent random variables which obeys the ξ distribution.

A PRCSG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers. The PRCSG is not truly random, because it is completely determined by the key *K*. We also can use chaos theory to design a PRCSG.

Then the encryption is done by the encryption function f,

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

The output encypted symbol sequence is $Y = \{y_1, y_2, ...\}$ whose *n*th element is y_n (a complex number), and y_n is a function of s_n and r_n. Here, $S = \{s_1, s_2, ...\}$ is a transmitted binary sequence. For *M*-ary modulation, s_n (the *n*th element of S) is a $\log_2 M$ length block of binary bits whose elements are "0" or "1".

Now f in (2) is the PLE function that we need to design. The design of f has two goals. One is to prevent eavesdroppers (without K) recovering any information from *Y*, and the other is to enable the legal receiver (with *K*) to effortlessly recover *Y*. We will later discuss in detail what kinds of f are best.

Returning to Fig.1, then after the cipher signal y_n passes through the channel, the symbols received at the legal receiver and the eavesdropper are respectively:

$$Z_B^n = H_B(y_n) \tag{3}$$

$$Z_E^n = H_E(y_n) \tag{4}$$

where $H_B(.)$ and $H_E(.)$ are the channel functions of Bob and Eve, respectively. The effects of channel noise are also included in $H_B(.)$ and $H_E(.)$.

2) Demodulation and decryption: The legal receiver Bob needs to recover S, knowing Z_B^n and K. In traditional communication systems, detection and decryption are two separate processes. However in PLE, the detection and decryption processes are combined together. We define the decryption and demodulation algorithm as:

$$\tilde{S} = \mathcal{D}(Z_B, K) \tag{5}$$

where $\mathcal{D}$ needs to be designed to reduce errors as much as possible. We also need to consider the computational complexity of $\mathcal{D}$.

C. Block PLE

Unlike stream PLE, block PLE processes a large chunk of data. Block PLE transforms large blocks of bits into complex vector signals with fixed or probabilistic functions. Probabilistic transformation means the output of PLE is a random variable. This is different from traditional block cipher with only fixed operations.

We model block PLE as a function that maps an *l*-bit binary vector into an *N*-length complex vector according to the key K:

$$\mathbf{S} = \{s_1 s_2 \dots s_l\} \xrightarrow{K} \mathbf{Y} = \{Y_1 Y_2 \dots Y_N\} \tag{6}$$

where $\mathbf{S}$ is a *l*-bit binary message block (i.e., different from stream PLE), K is the key whose length is k_l bits which also can be consider as an integer, and $\mathbf{Y} \in \mathbb{C}^{N\times 1}$ is the encrypted signal. Unlike stream PLE, l here is large (for example *l*=128, 256 or 512).

Let $\mathbf{F}_2$ denote the Galois field of two elements and let $\mathbf{F}_2^l$ denote the vector space of l tuples with elements in $\mathbf{F_2}$. We can represent block PLE as the following mapping T:

$$T : \mathbf{F}_2^l \times \mathbf{F}_2^{k_l} \to \mathbb{C}^N \tag{7}$$

where k_l is the key length.

Note that T is also allowed to be a stochastic mapping which is different from traditional cryptography.

We also can consider (6) as a family of operations with one parameter, and rewrite it as

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

The transformation T_K is the block PLE function which we need to design. We can see that the PLE function transforms the l-bit string S into a complex vector $\mathbf{Y}$ which is different from traditional cryptography in Shannon's work [1]. We call T pseudorandom if the function T_K(for a randomly-chosen key K) is indistinguishable from a function chosen uniformly at random from the set of all functions having the same domain and range.

Since the complex vector space is infinite, the theoretical key space of PLE is also infinite, while in conventional cryptography the key space is limited by the length of the message. So, PLE can naturally resist a brute-force attack.

D. Definitions of cryptographic primitives of the PLE system

An important work is to build cryptographic primitives for PLE. Only after PLE cryptographic primitives are well-established can it then be used to build practical cryptographic protocols for security systems. So we now give the definition of PLE *Cryptographic Primitives*.

Definition 2. Physical layer encryption system

Message space $\mathcal{M}$: the set of 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* between the transmitter and the receiver.

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

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

$\mathcal{H}$ 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 $Z_B \in \mathcal{Z}$.

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 $\{r_n\} = \{r_1, r_2, ...\} \in \mathbb{C}^n$.

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

There are some differences between PLE and conventional encryption.

1. The cipher signal space is different from conventional encryption. Here the cipher signal space $\mathcal{C}$ is a complex field.

2. The decryption algorithm requirements are different. Decoding errors are allowed in the PLE. In conventional encryption, it must be decoded correctly. In PLE, we only restrain the probability of the correct decryption as:

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

where δ_e is a given error threshold.

3. The encryption and decryption algorithms do not require deterministic functions. We can design them as random functions. In other words, the random function will give different outputs at different times even if the input is the same. This property can prevent many attacks such as Chosen-Plaintext Attacks (CPA).

4. The channel function is also a random factor in this system, due to random noise.

Finally, we can use the following formula to represent the cryptographic primitives of the PLE system:

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

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

III. The Design Framework and Rules of PLE

In this section we will be concerned with how to design PLE and propose the framework and rules of PLE. We should consider two aspects:

1. Reliability.

We need to ensure that the legal receiver can recover the transmitted signal easily and correctly. PLE must be able to counteract noise and channel effects. This requires that the encryption function guarantees the constellation distances after the transformation and that the superimposed channel noise is not amplified after decryption recovery.

2. Security

We should prevent eavesdroppers from recovering information. The encrypted signal shows confusion and diffusion, and uses the effects of the channel and noise to increase this confusion feature.

Reversibility and security are two different goals. When the PLE function has the greatest reliability, its confusion tends to decrease, so a trade-off needs to be made in the design. We will now discuss the design methods of stream PLE and block PLE.

A. Stream PLE Design Framework

The key module of the Stream PLE has two parts. One part is to generate a particular distribution of a complex random sequence based on the key K. Note that the random numbers here are not truly random, but rather a deterministic algorithm that can also be run at the legal receiver to obtain the same random complex sequence as the transmitter. The generation of pseudo-random complex numbers has been widely researched in many other works [14].

Another part is the design of the encryption function f in Fig. 2. In stream PLE, f is the mapping of a small number of bits to a complex number. To measure and guide the design of the f-function, we propose two indicators to measure reliability and confusion. Fixing the number of transmission bits and energy of the output signal *y*, we can use the following index parameters to evaluate the encryption function *f*.

a) Minimum constellation distance:

$$d = \min_{(i,j)i\neq j} |f(s_i - s_j, r_n)| \tag{9}$$

where s_i, $s_j \in \mathcal{M}$ are possible input messages and d is the minimum distance of two different messages. Note that d will eventually affect the bit error rate of the legitimate recipient. This indicator is similar to the constellation design indicator in traditional communication systems. We should design f to maximize *d*.

b) Distribution characteristics of the output signal: Note that if r 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 from a limited length key. So, r is a pseudo-random complex sequence and is not truly random. Therefore, eavesdroppers have the possibility of obtaining information about s or r 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:

$$H_e(Y) = -\iint_{-\infty}^{\infty} p(a,b)\log_2 p(a,b)dadb, \tag{10}$$

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 quantification accuracy). We thus have quantized entropy as:

$$H^{\Delta}(Y) := -\sum_{i=-\infty}^{\infty}\sum_{j=-\infty}^{\infty} \Gamma(i,j)\log_2 \Gamma(i,j), \tag{11}$$

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

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 $\mathcal{C}$ [15]. 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.

We now present two approaches for the design of the encryption function f.

(i) PLE based on traditional modulation

In transmitters, encryption transformation is performed after the traditional constellation mapping (such as BPSK, QPSK, 16QAM, etc.), and at the receiver decryption is performed before traditional constellation demodulation. The encryption and decryption transformation here needs to ensure that the constellation distance is not changed, in order to guarantee the error rate of the legal receiver.

In the phase modulation system (QPSK, BPSK, M-PSK, etc.), the generated θ_n follows the uniform distribution ($\theta \sim U[0,\ 2\pi]$). The input information bits are mapped by traditional M-PSK to obtain a complex symbol X_n, and then the following rotation processing is performed:

$$Y_n = X_n e^{\theta_n}. \tag{12}$$

Clearly the rotation in (12) leasves the distances between the constellation points unaltered (in accordance with the aforemention a) and b)). This method is used in [16] and [11].

(ii) New constellation for stream PLE

Instead of relying on existing modulation systems, the function f is totally redesigned so that the output Y is uniformly distributed in a given space.

For example, in our previous work [17], a 3-dimensional rotated constellation modulation was designed in which 2 bits are mapped to a 3-dimensional constellation point and evenly distributed on a spherical surface. These 3 dimensions in practical systems can be obtained by (for example) using the two dimensions of one subcarrier and one dimension form another subcarrier. For example, in an OFDM system 1.5 subcarriers can be combined to get an modulation unit.

First, each block of 2-bit data is mapped to the four vertices of the regular tetrahedron $\mathbf{X}_n \in \mathbb{R}^3$. The regular tetrahedron vertices have equal distances between them so the best performance can be obtained. Then the three-dimensional constellation is rotated to obtain an encrypted constellation $\mathbf{Y}_n \in \mathbb{R}^3$:

$$\mathbf{Y}_n = \mathbf{X}_n \cdot \mathbf{R}(\alpha,\beta,\gamma) \tag{13}$$

where $\mathbf{R}(\alpha,\beta,\gamma)$ is the rotation matrix in (14), and $\alpha,\beta,\gamma \sim U(0,2\pi)$ are random phase parameters. The distribution of

$$\mathbf{R}(\alpha,\beta,\gamma)=\begin{bmatrix}\cos\gamma & \sin\gamma & 0\\ -\sin\gamma & \cos\gamma & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & \cos\beta & \sin\beta\\ 0 & -\sin\beta & \cos\beta\end{bmatrix}\begin{bmatrix}\cos\alpha & \sin\alpha & 0\\ -\sin\alpha & \cos\alpha & 0\\ 0 & 0 & 1\end{bmatrix} \tag{14}$$

$\mathbf{Y}_n$ is shown in the Fig.3. These points are distributed on the surface of the sphere.

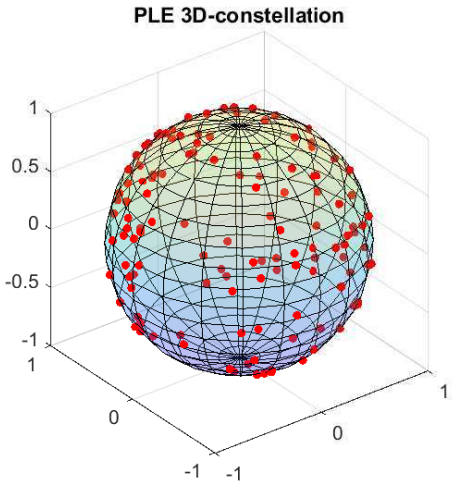

Fig. 3. PLE for a 3-D constellation where constellation points lie on the surface of the sphere with a uniform probability density function for each of the two parametric angles

B. Block PLE design framework

Block PLE operates on fixed-length groups of bits, called blocks, with a transformation that is specified by a symmetric key. Different from a traditional block cipher, block PLE converts bit blocks to complex vectors. Signals arriving at the receiver through the channel need to be correctly demodulated. So the rules of operation are very different from a traditional block cipher.

We need to design block PLE methods which should have the following properties.

(i) Confusion

Finding the relationship between the key and the cipher signal should be as complex and as involved possible. The key should be protected from exposure even when an attacker has large amounts of cipher signal to analyze.

(ii) Diffusion

The statistical structure of plaintext should be dissipated over the bulk of the cipher signal. There is no clear correspondence between plaintext and the cipher signal. This property ensures the PLE has the ability to resist differential attacks.

(iii) Noise tolerance

The cipher signal will pass through the wireless channel. When the signal-to-noise is large, the legal receiver should correctly recover the plaintext with a given key. In other words, decryption at the receiver should not increase the effect of the noise.

The framework of block PLE is shown in Fig. 4. A key schedule is an algorithm that expands a relatively short master key K to relatively different expanded keys (K_1, K_2, K_3) for

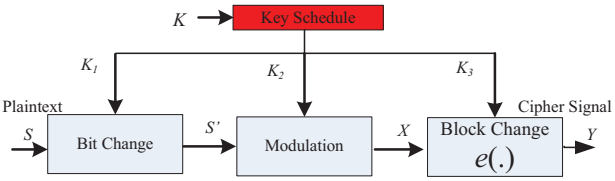

Fig. 4. Block PLE.

later use in an encryption algorithm [18]. We divide the steps of block PLE design into 3 phases: *Bit Change*, *Modulation* and *Block Change*. Each stage uses different keys, which are derived from the master key.

The bit change stage can use Boolean functions such as interleaving, substitution, permutation, etc. [19], [20]. The binary vector $\mathbf{S}$ is changed to $\mathbf{S}'$ according to K_1.

The modulation stage can use common modulation methods such as BPSK, QPSK, and 16 QAM, as well as a new multi-dimensional modulation method previously mentioned in section A:

$$\mathbf{S}'=\{s_1's_2'\dots s_l'\}\rightarrow\mathbf{X}=\{X_1X_2\dots X_N\}$$

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 stage in PLE. Essentially, it is a mapping function e in a complex vector space:

$$\mathbf{X}=\{X_1X_2\dots X_N\}\rightarrow\mathbf{Y}=\{Y_1Y_2\dots Y_N\} \tag{15}$$

$$\mathbf{Y}=e(\mathbf{X}) \tag{16}$$

where $\mathbf{Y}\in\mathbb{C}^N$ is the cipher signal vector. Here, we can design some sub-transforms e_1, e_2, e_3...and then combine them to form the final encryption transform.

$$e(\mathbf{X})=e_1(e_2(\dots(e_n(\mathbf{X})))). \tag{17}$$

Then, we consider what kind of functions can be used as sub-transforms for PLE.

a) Isometry transformation: First of all, let us consider the transformations which can guarantee the constant constellation distance. We will use the definition of isometry.

Definition 3. 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

$$d_Y(f(a),f(b))=d_X(a,b). \tag{18}$$

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

$$\mathbf{U}\mathbf{U}^{\mathrm{H}}=\mathbf{U}^{\mathrm{H}}\mathbf{U}=\mathbf{I}_N. \tag{19}$$

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 $(N^2 \times 1)$ given rotation direction vector $\mathbf{\Phi} \in \mathbb{R}^{N^2}$. Φ can be generated from K_3, 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 [21].

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

$$\mathbf{U} = e^{i\phi/2} \begin{bmatrix} e^{i\phi_1} \cos\theta & e^{i\phi_2} \sin\theta \\ -e^{-i\phi_2} \sin\theta & e^{-i\phi_1} \cos\theta \end{bmatrix}, \qquad (20)$$

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

Thus $e_i(\mathbf{X}) = \mathbf{UX}$ (see (17) for $e_i(\mathbf{X})$) can be used as a sub-transformation. We also can extend to $N > 2$ to acquire more confusion.

b) Stochastic transformation: If the eavesdropper can obtain a large number of plaintext and cipher signal pairs, then by only using an isometry transformation the system is likely to be cracked. In order to solve this problem and make the result of each encryption different, we need to introduce some stochastic transformations. These stochastic transformations make it impossible for an eavesdropper to perform a known-plaintext attack and so cannot calculate the encryption transform e from multiple accumulated Y and X data.

IV. Security Analysis and Performance comparison

A. Security analysis for KPA and CPA

On the eavesdropper side, we need Eve to be unable to recover S or K from Z_E.

We assume that Eve has the following characteristics:

1) Eve knows the channel functions $H_B(.)$ and $H_E(.)$.

2) Eve knows the PLE function f and the decryption function D, but does not know the secret key K.

Eve has the following attack aims:

1) Decode S from Z_E without knowledge of the key (ciphertext-only attack).

2) Recover K form Z_E with the known message S (known-plaintext attack).

3) Recover K form Z_E without the known message S (cipher text-only attack).

4) The enemy Eve can obtain the cipher signal for any specified plaintexts for the current key (chosen-plaintext attack).

The algorithm we design seeks to prevent these types of Eve attacks. From (4), 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 Z_E obtained will be different. S and Z_E do not show a one-to-one correspondence, which makes eavesdropper cryptanalysis methods such as linear attacks and differential analysis more difficult.

In block PLE systems, when designing $e(\mathbf{X})$, we need to ensure that even if Eve accumulates some plaintext and cipher signal pairs over a period of time, the function $e(.)$ cannot be inferred, and the key cannot be obtained. We consider the worst case where the noise $\mathbf{n}_E$ received by Eve is very small and can be ignored. Thus in the KPA situation, we assume that Eve can accurately obtain $\mathbf{Y}$.

In the phase rotation method [12], [13], [11], each nth 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 eavesdropper knows X_n and Y_n, then she 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, we encrypted the signal as a group. The unitary matrix $\mathbf{U}$ defined in the isometry transformation has $N \times N$ matrix elements, so that Eve cannot solve the 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. Thus, Eve cannot obtain $\mathbf{U}$ by accumulating $\mathbf{Y}$ and $\mathbf{X}$.

Note that in the stream PLE system, because r_n is changing all the time, its is obvious that KPA and CPA can be resisted by pseudorandom complex sequence generators.

B. Performance comparison of different PLE schemes

Due to page length constraints we can only directly summarize the performance of our two approaches (block PLE and stream PLE). A more thorough and detailed description will be presented later in a full journal paper.

In Table I we compare the performance of five different PLE schemes: phase rotation scheme [12], [13], [11], intrinsic interference scheme [9], sub-carrier obfuscate and dummy [8], our isometry based block PLE scheme, and our stream PLE framework. We consider five aspects: a) bit error ratio (BER) penalty, BER performance reduction due to PLE algorithm; b) throughput decrease; c) key space; d) CPA security, the ability to prevent CPA; e) encryption and decryption complexity.

As summarized in Table I, our scheme outperforms other PLE schemes. It is proven in the previous section that the phase rotation scheme cannot resist CPA, because this method encrypts symbol-by-symbol which does not obey the diffusion rule. 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. Actually, there are known attacks on stream ciphers. Also, the CPA security of the stream PLE framework is determined by PRCNG.

We also compared the encryption and decryption complexity of all the schemes. The main computational complexity in the isometry based block PLE scheme is a matrix multiplication. 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.

V. Conclusions

This paper established a general mathematical model and cryptography primitive of PLE. We divided the PLE into two types: stream PLE and block PLE. We proposed a framework and guidelines for designing stream PLE and block PLE. We proposed adopting an isometry transformation in PLE and introduced random functions to increase security against KPA and CPA. PLE has more cipher signal space and key space than traditional cryptography. Our proposed PLE frameworks provide more freedom in design and can resist KPA and CPA without any BER penalty.

TABLE I
PERFORMANCE COMPARISON OF DIFFERENT PLE SCHEMES.

	BER penalty	Throughput decrease	Key space	CPA security	Complexity
Phase rotation scheme [12], [13], [11]	No	No	High	No	$O(n)$
Intrinsic interference scheme [9]	1dB-4dB	No	High	No	$O(n)$
Subcarrier obfuscate and dummy [8]	No	$\alpha = k/(N_d s)$ *	High	Relies on stream cipher	$MO(n)$
Our isometry based block PLE	No	No	High	Good	$O(n)$
Our stream PLE framework	No	No	High	Relies on PRCNG	$O(n)$

* s is OFDM symbol number in one group, k is reserved subcarrier number for dummy data, and N_d is the subcarrier number [8].

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949. [Online]. Available: http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[4] 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 Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011.

[5] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, 2012.

[6] 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 Communications*, vol. 8, no. 16, pp. 2858–2862, 2014.

[7] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in mimo relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

[8] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an ofdm physical layer encryption scheme," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2114–2127, 2017.

[9] M. Sakai, H. Lin, and K. Yamashita, "Intrinsic interference based physical layer encryption for ofdm/oqam," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1059–1062, 2017.

[10] T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive mimo," *IEEE Transactions on Information Theory*, vol. 63, no. 8, pp. 5419–5436, 2017.

[11] 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.

[12] A. K. Nain, J. Bandaru, M. A. Zubair, and R. Pachamuthu, "A secure phase-encrypted ieee 802.15.4 transceiver design," *IEEE Transactions on Computers*, vol. 66, no. 8, pp. 1421–1427, 2017.

[13] 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.

[14] J. E. Gentle, *Random number generation and Monte Carlo methods*. Springer Science & Business Media, 2006.

[15] T. M. Cover and J. A. Thomas, *Elements of InformationTheory*. John Wiley & Sons, 1991.

[16] G. S. Kanter, D. Reilly, and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Communications Magazine*, vol. 47, no. 11, pp. 74–81, 2009.

[17] X. Li, W. Li, J. Lei, and L. Cheng, "A novel physical layer encryption algorithm based on three dimensional constellation rotation in ofdm system," *Acta Electronica Sinica*, vol. 45, no. 12, p. 2873, 2017, in Chinese.

[18] J. Kelsey, B. Schneier, and D. Wagner, "Key-schedule cryptanalysis of IDEA, g-DES, GOST, SAFER, and triple-DES," in *Advances in Cryptology — CRYPTO '96*. Springer Berlin Heidelberg, 1996, pp. 237–251.

[19] T. W. Cusick and P. Stanica, *Chapter 7 - Block ciphers*. Boston: Academic Press, 2009, pp. 157–191.

[20] M. A. Khan, M. Asim, V. Jeoti, and R. S. Manzoor, "On secure ofdm system: Chaos based constellation scrambling," in *2007 International Conference on Intelligent and Advanced Systems*. IEEE, Nov. 2007, Conference Proceedings, pp. 484–488.

[21] D. Mortari, "On the rigid rotation concept in n-dimensional spaces," *Journal of the Astronautical Sciences*, vol. 49, Jul. 2001.