Multi-dimensional Encryption Scheme based on Physical Layer for Fading Channel

Ying Huang[1*], Jing Lei[1], Mohammed El-Hajjar[2], Wei Li[1]

[1]Institute of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, Hunan Province, P. R. China

[2]Department of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, United Kingdom

[*]corresponding. inform_huang@sina.com

Abstract — In order to solve the security problem for fading channel, a pragmatic physical layer encryption (PLE) scheme is proposed, which utilizes diversity technique elaborately. Different from the conventional PLE schemes based on phase rotation for modulated symbol, the proposed scheme changed phase and amplitude together for a block of symbols each time, which can be defined as multi-dimensional PLE (MPLE). Unconventional constellation obfuscates eavesdropper, which can be seen as the first level security in physical layer. The correct probability based on chosen plaintext attacks (CPA) and known plaintext attacks (KPA) are deduced. It can be seen from the simulation results that the MPLE scheme can achieve lower attack success probability because of multi-level security and better performance based on diversity under fading channel.

1. Introduction

In wireless communication, broadcast nature makes it difficult to shield transmitted signals from unintended recipients, while channel fading leads to performance decrease seriously. How to achieve security and reliability under wireless fading channel is popular these years. Different from traditional security scheme (encryption, authentication .etc.), the physical layer security (PLS) has attracted research attention recently. As the lowest layer of the protocol stack, it has several advantages including: having the lowest impact on the network, having low latencies and introducing no overhead. In recent years, more research focus has been put towards physical layer encryption (PLE), where the encryption is added in physical layer with the secret key extracted from channel based on its randomness and reciprocity.

Some PLE schemes are based on conventional encryption, in which the encoded message is encrypted before modulation. A. Zuquete *et.al.* [1] have discussed the approach of PLE using a classical stream cipher, which can be used effectively against known-plaintext attacks (KPA) because of the natural randomness of the noisy communication channel. Ahmad *et.al* [2]added encryption after error coding and interleaving, while using the well proven secure AES (Advanced Encryption Standard) algorithm as a key stream generator. In the architecture of[2] , the whole MAC (Media Access Control) frame was encrypted and the robust location privacy could be achieved. G. S. Kanter *et.al.* [3, 4] discussed the security scheme in optical communication with traditional cryptography. The PLE schemes proposed in literature [1-4] are applied before modulation, where bit-stream operations are employed.

On the other hand, some PLE schemes are based on distorting the modulated symbols, in which the encryption is performed after modulation. M. Tahir *et.al.* [5] enhanced the security by distorting the original signal constellation based on encryption and channel pre-compensation, which makes the estimation of the constellation and modulation type difficult. The proposed PLE schemes in [6, 7] randomize the radio signal using a secret key extracted from the main channel under the assumption of channel reciprocity and using a discrete Fourier transform (DFT) based encryption algorithm, respectively. F. Huo *et.al.*[8] compared XOR encryption and phase encryption in terms of their security and encryption efficiency, where it was shown that phase encryption can resist traffic analysis attack when implemented in the physical layer. Zhijiang XU *et.al.*[9] proposed a PLE scheme based on random rotation of the modulated symbol using chaotic sequence.

Especially in some schemes, the characteristics of orthogonal frequency division multiplexing (OFDM) signals are destroyed in order to enhance the security. G. Baojian *et.al*. [10] used a secret seed key to control the phase rotation factor and amplitude size of traditional modulation (PSK/QAM), which disrupts the OFDM constellation mapping process. Hence, using these techniques, modulation protection can be achieved. Furthermore, a PLE algorithm for Discrete Fourier Transform Spread OFDM (DFT-S-OFDM) was proposed in [11]. The algorithm utilizes a random key to produce two complex diagonal key matrices, multiplied by the two matrices respectively before and after the N-point DFT transform, which can resist brute-force attack and plaintext cipher-text attack. Manabu Sakai *et.al.*[12] proposed a PLE method for OFDM/OQAM, which use intrinsic interferences of added pure imaginary symbols to obfuscate true data symbols at the eavesdroppers.

Masking operation is also used in some PLE schemes. A. Chorti [13] proposed the use of non-orthogonal FDM signals to mask the information bearing OFDM signal, which results in the OFDM signal becoming practically undetectable by a potential eavesdropper. F. Huo *et.al.* [14] proposed a PLE scheme through destroying the orthogonality of OFDM symbols, which creates intercarrier interferences. The encryption performed on the time domain OFDM symbols is equivalent to performing nonlinear masking in the frequency domain [14]. Eric Tollefson *et.al.*[15] proposed a practical PLE approach through spatial masking for out-phased array linearized signaling (OPALS). It modified the transmitter to employ the outphasing amplifier design to generate a unique masking signal to each element of an antenna array.

Up to now, there are still two problems in the research of PLE schemes: 1) The tradeoff between security and reliability; 2) How to cope with the negative influence of channel condition. In this paper, we will discuss the pragmatic solution for these two problems. For wireless communication, fading seriously influences the transmission quality. Diversity is a traditional technique to combat fading. We propose a novel PLE scheme based on modulation diversity to achieve security and reliability, the contributions of the paper are summarized as follow:

1) A multi-dimensional physical layer encryption (MPLE) scheme is proposed, which changes both phase and amplitude of a block of modulated symbols. Based on the merit of diversity technique, MPLE scheme can achieve security as well as combating fading.

2) We discuss the encryption and decryption of MPLE in detail, where the decryption is united with iterative demodulation and decoding. Furthermore, the performance under fading channel is analyzed.

3) We analyze the security based on attacks from the view of communication receiver of eavesdroppers, and deduce the attack success probability of chosen plaintext attacks (CPA) and KPA.

4) We evaluate the performance of MPLE scheme based on attack success probability and bit error rate (BER) performance under fading channel. Furthermore, we discuss the comparison between MPLE scheme and other PLE schemes at the performance penalty for security.

The rest of this paper is organized as follows. The next section presents the preliminaries and background. And the system model is shown in Section 3. The proposed MPLE scheme is discussed detailed in Section 4, which includes encryption, united decryption with iterative demodulation and decoding, and the performance analysis under fading channel. The security of the proposed scheme will be analyzed in Section 5. Performance evaluations are presented in Section 6. Finally, Section 7 presents our conclusions and final comments.

2. Preliminaries and Background

2.1 Preliminaries

The followings are a list of notations which will be used throughout the paper.

- We use lowercase and bold letters or uppercase letters to denote vectors or sequences as follows, $\boldsymbol{s} = [s_1, s_2, ...]$.
- We use uppercase and bold letters to denote a matrix, i.e. $\boldsymbol{G}$.
- $\boldsymbol{A}^T$ denotes the transpose matrix.
- $\boldsymbol{A}^H$ denotes transposed and complex conjugated matrix (Hermitian).
- $\|\bullet\|$ denotes matrix norm.
- $|\bullet|$ denotes the absolute value.
- $\otimes$ denotes element-by-element multiplication. For example, $C = A \otimes B$ means that multiplies vectors A and B element-by-element and returns the result in C. Inputs A and B must have the same size.

2.2 Background

1)Modulation diversity

Modulation diversity(MD), also known as signal space diversity, can provide performance improvement over fading channels by increasing the diversity order of a communication system. Modulation diversity can also be seen as multi-dimensional rotated constellations[16]. The rotation was employed after modulation mapping, and the approximate performance can achieve near-Gaussian performance when communicating over fading channels without any power or bandwidth expense. More detailed discussion can be found in [17-19].

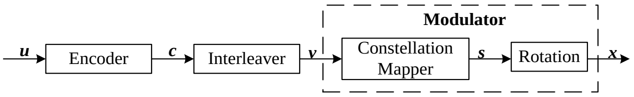


Fig.1.*Block diagram of the transmitter with constellation rotation*

The general block diagram of the transmitter with constellation rotation is shown in Fig. 1 [20]. The information sequence $\boldsymbol{u}$ is first encoded into a coded sequence $\boldsymbol{c}$. The coded sequence $\boldsymbol{c}$ is then interleaved by a bit-wise interleaver to produce the interleaved sequence $\boldsymbol{v}$. Assume that each complex component of a complex N-dimensional constellation carries m coded bits. Hence, a sequence of Nm coded bits is mapped to one complex N-dimensional constellation symbol at the modulator to produce the symbol sequence $\boldsymbol{s} = [s_1, s_2, ..., s_N]$, where $s_i \in \psi$, $\forall i$, with ψ being the conventional constellation. The symbol sequence $\boldsymbol{s}$ is then rotated by an $N \times N$ complex rotation matrix $\boldsymbol{G}$, which forms sequence $\boldsymbol{x} = [x_1, x_2, ..., x_N]$. The essence of rotation can be written by e.g(1) as follow

$$\boldsymbol{x} = \boldsymbol{s} \cdot \boldsymbol{G} \quad (1)$$

The space of the rotated sequence $\boldsymbol{x}$ is the new constellation, which is denoted by Ψ. If $|\psi| = 2^m$, then $|\Psi| = 2^{Nm}$. Ψ is N-dimensional constellation, which depends on $\boldsymbol{G}$ and ψ.

MD can achieve higher diversity order, which is equal to the minimum number of distinct components between any two N -dimensional constellation elements. The entries $g_{i,j}, 1 \le i, j \le N$, of $\boldsymbol{G}$ satisfy the following power constraint:

$$\sum_{i=1}^{N} \sum_{j=1}^{N} \left\| g_{i,j} \right\|^2 = N \tag{2}$$

2) Conventional encryption and PLE

The conventional encryption is key-based, which is used at the upper layers (such as application and network layers). For example, in encryption of stream cipher, key stream is bitwise XORed with the information bits in order to produce the ciphertext. The decryption is also processed in the same layer. In general, its security relies on the infeasible computational complexity at the decoding operation for the eavesdropper. Nowadays, data encryption standard (DES) and AES are both widely used encryption techniques.

Unlike the conventional encryption, PLE is the encryption process performed in the physical layer, which can be added after channel coding or modulation. It makes use of all kinds of characteristics of the signal to design the encryption scheme. The operation can be used at the bit level or at the symbols level. The secret key is always extracted from the random channel, which can be shared by legitimate communication pair based on the reciprocity of channel. PLE is the technique in PLS.

3)Secrete key generation

The traditional wiretap channel model comprises transmitter, legitimate receiver and eavesdropper. It assumed that the secret key is generated based on physical layer channel characteristics (such as received signal strength, phase information etc.). Under the recent techniques, we can assume that: 1) The legitimate channel is independent with the wiretap channel; 2) The secrete key is identical between the transmitter and the legitimate receiver based on channel reciprocity; 3) The key is generated at the beginning of each transmission. We only discuss the PLE scheme in this paper, not including key generation from the channel.

3. System Model

We consider a system with two points: transmitter and receiver. Transmission is performed over Time Duplex Division (TDD) channels. At any transmission time, the received signal can be expressed as follows

$$\boldsymbol{y} = \boldsymbol{h} \otimes \boldsymbol{x} + \boldsymbol{n} \tag{3}$$

where $\boldsymbol{h} = \left[h_1, h_2, \ldots \right]$ is the fading channel coefficients, which is independent and identically distributed (i.i.d) with $E[h_i^2] = 1$. $\boldsymbol{n}$ is the Additive White Gaussian noise with variance σ^2. Without loss of generality, we assume that coherent detection is used and the phase changes due to fading effect are perfectly recovered at the receiver. Furthermore, the fading coefficients can be simply modeled as independent scalar Rayleigh random variables with unit mean square.

At the beginning of each transmission time, the instantaneous channel characteristics are estimated using pilot signals in the same time slot or two consecutive time slots. The channel phase ϕ is uniformly distributed in the interval $[0, 2\pi]$. We can divided $[0, 2\pi]$ into Q equal intervals, which index can be denoted as $\left[1, 2, 3, \ldots, Q\right]$. The constant Q is already known by transmitter and receiver. The index of the interval, which phase ϕ is in, can be seen as the secret key $\boldsymbol{K}$. Using channel reciprocity principles, the secret key based on instantaneous channel characteristics is shared by two legitimate points. It is worth noticing that the channel phase for each transmission is independent from previous transmission.

4. Proposed PLE Scheme

Based on the description of modulation diversity technique in Section 2.2, the size of conventional constellation ψ is 2^m. However, the size of rotated constellation Ψ is 2^{Nm} ($N \geq 2$). Compared with conventional constellation, the size of multi-dimensional constellation grows exponentially with the dimension value N . Hence, the rotation operation of e.g.(1) disorganizes the location of constellation points in ψ , and makes it more difficult for the eavesdropper to attack with the conventional methods. Furthermore, constellation rotation provides a diversity gain, which results in performance improvement in fading channels. That is to say, modulation diversity technique can be used in communications system for security and reliability simultaneously, which is the core of the proposed PLE scheme.

Fig. 2 shows the communication system with proposed PLE scheme. The encoder, interleaver (Π) and constellation mapping are combined as a conventional bit-interleaved coded modulation (BICM) system. Then, symbol sequence is serial-to-parallel converted to multi-dimensional symbol vectors. Each vector will be rotated based on secret key $\boldsymbol{K}$, which is extracted from channel. We won't discuss key generation based on channel in this paper, and assume that the same key is known by both legitimate users. It is worth noticing that secrete key generation is done at the beginning of each transmission, and will be kept invariable at the whole transmission. Furthermore, transmitter and legitimate receiver have the same random number generator, which is unknown by eavesdroppers.

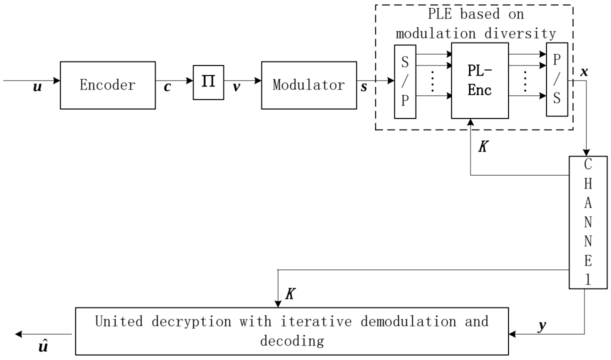


Fig.2. *The proposed PLE scheme based on modulation diversity*

4.1 Encryption

$\boldsymbol{K}$ can be seen as the seed of random number generation. We use $\boldsymbol{K}$ to generate the random sequence $\boldsymbol{G} = [\boldsymbol{g}_1 \boldsymbol{g}_2 \cdots \boldsymbol{g}_N]$, where $\boldsymbol{g}_j = \begin{bmatrix} g_{1,j} & g_{2,j} & \cdots & g_{N,j} \end{bmatrix}^T$. Let $\boldsymbol{s} = [s_1, s_2, \ldots]$ be the modulated symbol sequence and $\boldsymbol{x} = [x_1, x_2, \ldots]$ be the encrypted symbol sequence as shown in Fig.2. After serial-to-parallel conversion of the symbol sequences, each N symbols are encrypted with random sequence $\boldsymbol{G}$ to form a N -dimensional encrypted symbol, where the encryption algorithm is shown in Fig. 3. For general PLE schemes, distortion is added on each modulated symbol. In our scheme, a block of modulated symbol is distorted together, where the symbols can be affected by each other in the same block. So that, the proposed PLE scheme can be defined as the multi-dimensional PLE (MPLE) scheme. The constellation of encrypted symbols will be distorted badly. Furthermore, it is worth noticing that $\boldsymbol{G}$ will not be changed in whole transmission, and variant from different transmissions.

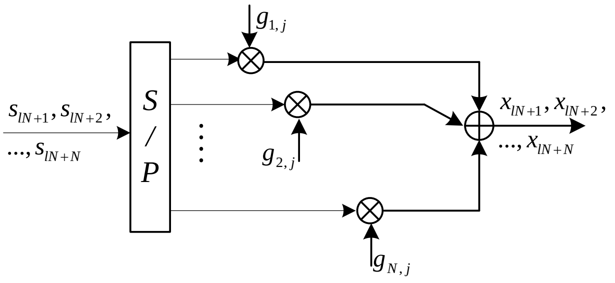


Fig.3. *Encryption algorithm of MPLE*

We divide the symbol sequence $\boldsymbol{s}$ into several blocks with N symbols each, and the l -th block can be denoted as $\left[s_{lN+1}, s_{lN+2}, \cdots, s_{lN+N}\right]$. From Fig.3, the encryption can be described as follows:

$$x_{lN+j} = \sum_{i=1}^{N} g_{i,j} \cdot s_{lN+i}$$

$$\text{(for } j\text{=1,2,…}N\text{; and } l = 0,1,\ldots) \qquad (4)$$

The l -th N -dimensional encrypted symbol is $\left[x_{lN+1}, x_{lN+2}, \cdots, x_{lN+N}\right]$. It can be seen from e.g.(4) that each encrypted symbol x_{lN+j} is the weighted combination of $\left[s_{lN+1}, s_{lN+2}, \cdots, s_{lN+N}\right]$, and the weight coefficients are selected from $\boldsymbol{G}$ in sequence.

$\boldsymbol{G}$ should obey the following rules :

1) Power constraint, i.e. $\left\|\boldsymbol{g}_j\right\|^2 = 1$.

2) Equivalent amplitude, i.e. $\left|g_{ij}\right|^2 = 1/N$.

3) Independence and randomness of $\boldsymbol{g}_j$.

Rule 1) is to control the transmitted power and rule 2) is for equal error protection. Rule 3) ensures that the selection of $\boldsymbol{g}_j$ is independent and random. E.g.(4) can also be written as follow

$$\left[x_{lN+1} \quad x_{lN+2} \quad \cdots \quad x_{lN+N}\right] = \left[s_{lN+1} \quad s_{lN+2} \quad \cdots \quad s_{lN+N}\right] \cdot \boldsymbol{G}$$

$$\boldsymbol{x} = \boldsymbol{s} \cdot \boldsymbol{G} \qquad (5)$$

Taking into account the practicality, rule 3) can be changed to rule 4) as follow

4) $\boldsymbol{G}$ is full-rank , i.e. $\left|\boldsymbol{G}\right| \neq 0$.

Essentially, the MPLE scheme is equivalent to the multi-dimensional constellation rotation, in which $\boldsymbol{G}$ is the rotation matrix with $g_{i,j}$ ($i = 1,\ldots,N;\ j = 1,\ldots,N$) as its entries. Under the premise of satisfying the above basic rules, we show the generation algorithm of rotated matrix $\boldsymbol{G}$.

Algorithm 1: rotated matrix $\boldsymbol{G}$ generation

(1) Partition [0,1] into $N \times N$ intervals uniformly, and the index of intervals is denoted as (1,2,…, $N \times N$).

(2) Using key $\boldsymbol{K}$ as a seed to generate a random number a in [0,1], which obeys uniform distribution.

(3) Check a , and decide which interval is in, then output the index of the interval as $i_{kj}(k, j = 1,\ldots,N)$.

(4) Repeat (1)~(3), the random integer matrix $I_{N\times N}$ can be formed, where i_{kj} is the entities.

(5) Construct $\boldsymbol{G}$ as e.g.(6) based on random matrix $I_{N\times N}$, where A is a constant larger than $\frac{N\times N}{2}$.

$$\boldsymbol{G} = \frac{1}{\sqrt{N}} \begin{bmatrix} \exp\left(j\frac{\pi i_{11}}{A}\right) & \exp\left(j\frac{\pi i_{12}}{A}\right) & \cdots & \exp\left(j\frac{\pi i_{1N}}{A}\right) \\ \exp\left(j\frac{\pi i_{21}}{A}\right) & \exp\left(j\frac{\pi i_{22}}{A}\right) & \cdots & \exp\left(j\frac{\pi i_{2N}}{A}\right) \\ \vdots & \vdots & \cdots & \vdots \\ \exp\left(j\frac{\pi i_{N1}}{A}\right) & \exp\left(j\frac{\pi i_{N2}}{A}\right) & \cdots & \exp\left(j\frac{\pi i_{NN}}{A}\right) \end{bmatrix} \quad (6)$$

(6) Check $\left|\boldsymbol{G}\right| \neq 0$. If not, go back to (1) and regenerate.

Example 1: Let $N = 3$, $A = 18$, two rotated matrixes are generated as follow:

$$\boldsymbol{G}_1 = \frac{1}{\sqrt{3}} \begin{bmatrix} \exp\left(j\frac{4\pi}{18}\right) & \exp\left(j\frac{9\pi}{18}\right) & \exp\left(j\frac{8\pi}{18}\right) \\ \exp\left(j\frac{6\pi}{18}\right) & \exp\left(j\frac{8\pi}{18}\right) & \exp\left(j\frac{4\pi}{18}\right) \\ \exp\left(j\frac{\pi}{18}\right) & \exp\left(j\frac{7\pi}{18}\right) & \exp\left(j\frac{6\pi}{18}\right) \end{bmatrix}$$

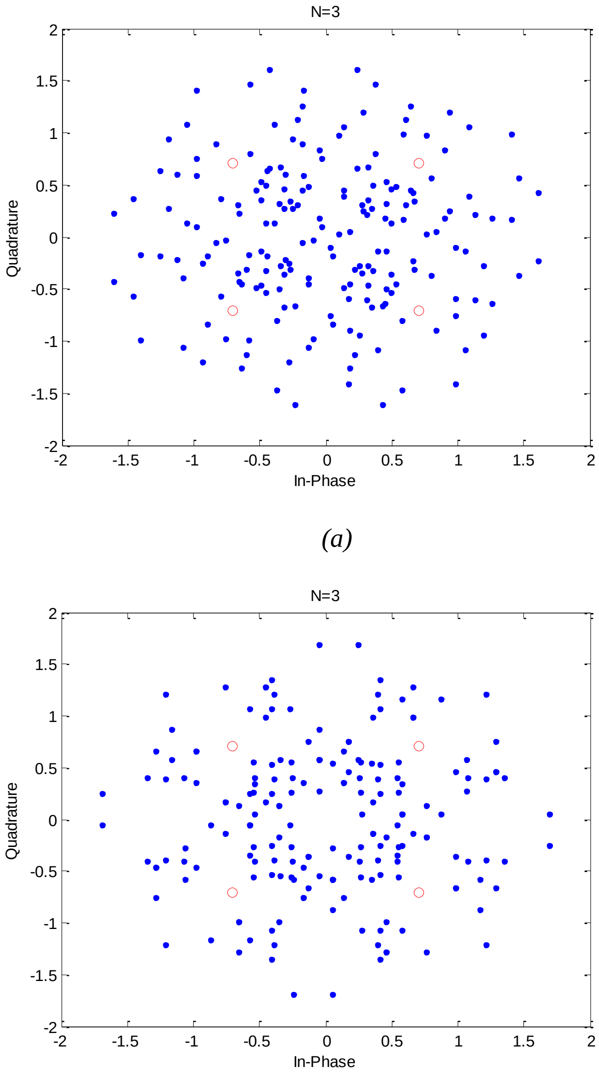
$$\boldsymbol{G}_2 = \frac{1}{\sqrt{3}} \begin{bmatrix} \exp\left(j\frac{6\pi}{18}\right) & \exp\left(j\frac{3\pi}{18}\right) & \exp\left(j\frac{8\pi}{18}\right) \\ \exp\left(j\frac{5\pi}{18}\right) & \exp\left(j\frac{5\pi}{18}\right) & \exp\left(j\frac{9\pi}{18}\right) \\ \exp\left(j\frac{3\pi}{18}\right) & \exp\left(j\frac{3\pi}{18}\right) & \exp\left(j\frac{\pi}{18}\right) \end{bmatrix}$$

Example 2: Let $N = 4$, $A = 32$, two rotated matrixes are generated as follow:

$$\boldsymbol{G}_3 = \frac{1}{\sqrt{4}} \begin{bmatrix} \exp\left(j\frac{9\pi}{32}\right) & \exp\left(j\frac{2\pi}{32}\right) & \exp\left(j\frac{13\pi}{32}\right) & \exp\left(j\frac{11\pi}{32}\right) \\ \exp\left(j\frac{2\pi}{32}\right) & \exp\left(j\frac{16\pi}{32}\right) & \exp\left(j\frac{9\pi}{32}\right) & \exp\left(j\frac{3\pi}{32}\right) \\ \exp\left(j\frac{13\pi}{32}\right) & \exp\left(j\frac{\pi}{32}\right) & \exp\left(j\frac{15\pi}{32}\right) & \exp\left(j\frac{4\pi}{32}\right) \\ \exp\left(j\frac{16\pi}{32}\right) & \exp\left(j\frac{11\pi}{32}\right) & \exp\left(j\frac{15\pi}{32}\right) & \exp\left(j\frac{3\pi}{32}\right) \end{bmatrix}$$

$$G_4 = \frac{1}{\sqrt{4}}\begin{bmatrix} \exp\left(j\frac{\pi}{32}\right) & \exp\left(j\frac{6\pi}{32}\right) & \exp\left(j\frac{11\pi}{32}\right) & \exp\left(j\frac{11\pi}{32}\right) \\ \exp\left(j\frac{2\pi}{32}\right) & \exp\left(j\frac{7\pi}{32}\right) & \exp\left(j\frac{16\pi}{32}\right) & \exp\left(j\frac{4\pi}{32}\right) \\ \exp\left(j\frac{10\pi}{32}\right) & \exp\left(j\frac{16\pi}{32}\right) & \exp\left(j\frac{13\pi}{32}\right) & \exp\left(j\frac{5\pi}{32}\right) \\ \exp\left(j\frac{16\pi}{32}\right) & \exp\left(j\frac{16\pi}{32}\right) & \exp\left(j\frac{6\pi}{32}\right) & \exp\left(j\frac{11\pi}{32}\right) \end{bmatrix}$$

The corresponding constellation is shown in Fig.4 and Fig.5 respectively.

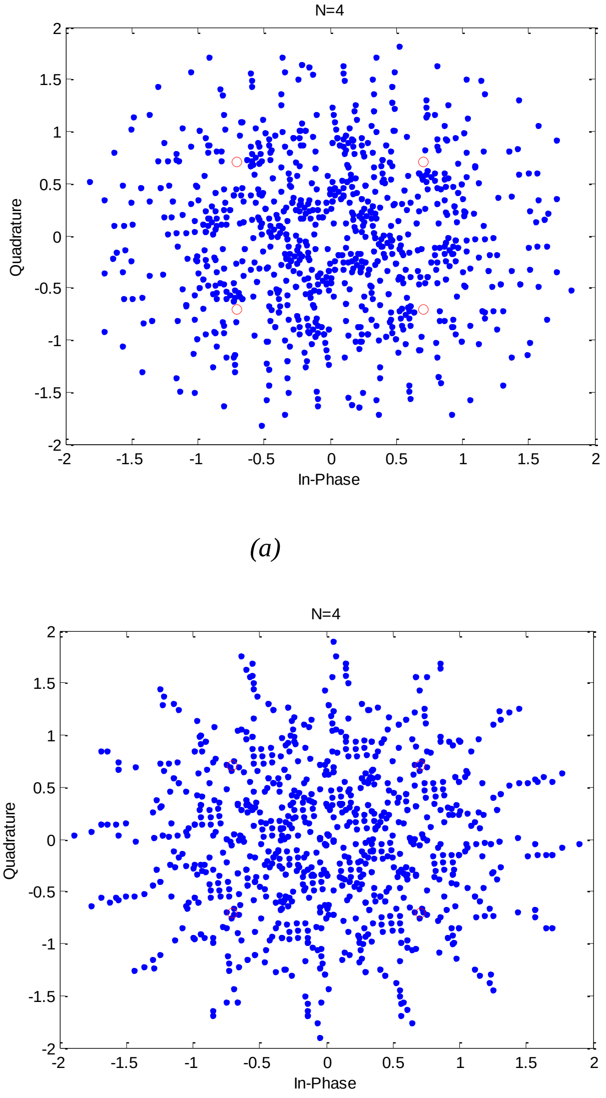


(a)

(b)

Fig.4 *The equivalent constellation with N=3*

(a) G$_1$ (b)G$_2$



(a)

(b)

Fig.5. *The equivalent constellation with N=4*

(a) *G*$_3$ (b)*G*$_4$

The red circle in Fig.4 and Fig.5 are the signal of the original constellations. It can be seen from the figures that the signal of the encrypted constellation is rotated and scattered, which is changed in both phase and amplitude.

Based on above MPLE scheme, there are three levels in security as follow:

Level 1: the dimension N ;

Level 2: the structure of rotated matrix $\boldsymbol{G}$ such as e.g.(6), and the constant A ;

Level 3: the random integer matrix $I_{N\times N}$ based on secret key $\boldsymbol{K}$.

In our MPLE scheme, channel phase ϕ is variant in each transmission, which leads to different $\boldsymbol{K}$ and $\boldsymbol{G}$. Though one-time-pad encryption scheme is impractical in traditional encryption because of the key space, our scheme is a practical solution based on channel randomness.

4.2 United decryption with iterative demodulation and decoding

In the communication system, it is assumed that coherent detection is used and the phase changes due to fading effect are perfectly recovered at the receiver. In the MPLE scheme, decryption is not equivalent to $\boldsymbol{G}^{-1}$. In order not to lower the performance because of the noise, we can combine decryption with iterative demodulation and decoding[20], which is shown as Fig.6. The receiver is based on a BICM-ID system, which includes the soft-input soft-output (SISO) demodulator (Demod) , the SISO channel decoder (SISO Dec), interleaver (Π) and deinterleaver (Π^{-1}).

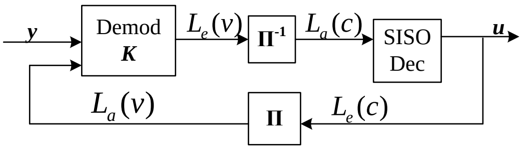


Fig.6. *Block diagram of the process at receiver*

Because of channel reciprocity, phase ϕ is identical at transmitter and legitimate receiver. That is to say, $\boldsymbol{K}$ and $\boldsymbol{G}$ are known by legitimate receiver. We can first use $\boldsymbol{G}$ to construct the rotated multi-dimensional constellation Ψ ($|\Psi|=2^{Nm}$), where Nm -bit labeling corresponds to N -dimensional symbol. Then, the constellation Ψ is used in the demodulation. Hence, we call it united decryption with iterative demodulation and decoding.

Based on the SISO demodulation algorithm in[21, 22] , we can use the modified algorithm as shown in e.g.(7), which uses constellation Ψ to substitute the conventional constellation ψ .

$$L_e(v_i) = \ln \frac{\sum\limits_{\mathbf{v}\in\chi_i^1} P(\boldsymbol{y}\,|\,\boldsymbol{x}) \exp \sum\limits_{\substack{j=1,\, j\neq i \\ v_j=1}}^{Nm} L_a(v_j)}{\sum\limits_{\mathbf{v}\in\chi_i^0} P(\boldsymbol{y}\,|\,\boldsymbol{x}) \exp \sum\limits_{\substack{j=1,\, j\neq i \\ v_j=0}}^{Nm} L_a(v_j)} \qquad (7)$$

where $L_a(c)$ and $L_a(v)$ are the a priori log likelihood ratio (LLR) for the decoder and the demodulator, respectively. $L_e(c)$ and $L_e(v)$ are extrinsic LLRs from the decoder and the demodulator, respectively. χ_i^b $(b=0,1)$ is a subset belonging to the rotated constellation Ψ, in which the i -th bit of all signal labels is b and the size of each subset χ_i^b is $2^{Nm/2}$. Compared with the conventional BICM-ID system, the additional time complexity of the MPLE scheme is $\boldsymbol{O}(2^{mN})$, which lies in the demodulation based on multi-dimensional constellation Ψ .

4.3 Performance analysis under fading channels

The average pairwise error probability of the MPLE system can be written as

$$f\left(d,\Psi,\xi_\Psi\right) \leq \Phi^d(\Psi,\xi_\Psi)$$

$$= \left\{ \frac{1}{Nm2^{Nm}} \sum_{\boldsymbol{s}\in\Psi} \sum_{k=1}^{Nm} \left[\prod_{j=1}^{N} \left(1 + P \frac{\left\| \boldsymbol{g}_j \cdot (\boldsymbol{s}-\boldsymbol{s}') \right\|^2}{4\sigma^2} \right)^{-1} \right] \right\}^d \qquad (8)$$

where $\boldsymbol{g}_j$ is the j -th column of $\boldsymbol{G}$, d is the Hamming distance of the channel code used, P is the transmitted power, Ψ is the rotated constellation after multi- dimensional encryption, and $|\Psi|=2^{Nm}$. ξ_Ψ is the labeling rule based on Ψ . $\boldsymbol{s}$ and $\boldsymbol{s}'$ are any two multi-dimensional symbols with only the k -th bit of their label is different.

Based on e.g.(8), we can conclude that Nd-order diversity can be achieved with the well-designed $\boldsymbol{G}$. It means that the proposed MPLE scheme can achieve diversity gain, which can cope with the fading in the channel.

5. Security Analysis

In MPLE scheme, transmitter rotates their symbol vector using matrix $\boldsymbol{G}$, which is unknown to the eavesdroppers. Furthermore, it also takes into account the contribution of the channel noise to the system's security. In this section, we present security analysis form the communication receiver of eavesdroppers.

5.1 The attacks based on communication receiver

From the view of communication receiver, the eavesdropper can use the conventional methods to analyze the signal after detecting the signal from the transmitter, which includes carrier estimation, symbol rate estimation, modulation recognition, channel codes recognition, etc. Because of the unconventional constellation in MPLE scheme, it is harder for the eavesdropper to recognize the modulation, which can achieve the first protection.

From the e.g.(4), the encrypted symbol is the combination of N original symbols selected from the conventional constellation, which is changed in both phase and amplitude. In this case, the conventional recognition methods, such as instantaneous characteristics or cumulant characteristics, are useless.

Cumulant-based classification[23, 24] is more robust for modulation recognition. In this part, we discuss the blind recognition problem of encrypted constellation based on cumulants with second-order moments (C_{20}, C_{21}), fourth-order moments (C_{40}, C_{41}, C_{42}) and sixth-order moments (C_{60}, C_{63}). The theoretical values for conventional constellation and rotated constellation are described in Table I, which are obtained by computing the ensemble averages over the ideal noise-free constellation under the constraint of unit energy. From Table 1, it can be seen that the theoretical cumulant values of rotated constellation are different from the original values. Therefore, it is difficult to recognize the modulation correctly. That is to say, the correct recognition probability will be decreased, which leads to the receive signal incorrectly.

Table 1 Theoretical Cumulant Statistics Values for Conventional Constellation and Rotated Constellation

Modu	QPSK			16QAM		
	orignal	N=3	N=4	orignal	N=3	N=4
$\lvert C_{20}\rvert$	0	0	0	0	0	0
$\lvert C_{21}\rvert$	1	1	1	1	1	1
$\lvert C_{40}\rvert$	1	0	0	0.68	0	0
$\lvert C_{41}\rvert$	0	0	0	0	0	0
$\lvert C_{42}\rvert$	1	0.33	0.25	0.68	0.22	0.17
$\lvert C_{60}\rvert$	0	0	0	0	0	0
$\lvert C_{63}\rvert$	4	0.44	0.25	2.08	0.23	0.13

5.2 Chosen Plaintext Attacks (CPA)

The dimension N is unknown by eavesdroppers, which can be seen as the first level security in MPLE scheme. Before CPA, N should be decided by random guessing in $[2, N_{\max}]$, where $N_{\max}$ is the maximum dimension value. As shown in Section 4, larger N leads to higher complexity. That means N can't be too large in application. Generally, $N_{\max}$ will not larger than 32[20]. Under these circumstances, the correct guessing probability is $1/(N_{\max}-1)$.

the received signal of eavesdroppers can be written as

$$\boldsymbol{y} = (\boldsymbol{h} \otimes \boldsymbol{s}) \cdot \boldsymbol{G} + \boldsymbol{n} \qquad (9)$$

In CPA, we assume that adversary can request N transmissions of a chosen information signal $\boldsymbol{s}$, that is

$$\boldsymbol{s}_1 = [1 \quad 0 \quad \cdots \quad 0], \ldots, \boldsymbol{s}_N = [0 \quad 0 \quad \cdots \quad 1] \quad (10)$$

For a certain value N

$$\boldsymbol{s}_1\boldsymbol{G} = [g_{11} \quad g_{12} \quad \cdots \quad g_{1N}] = \boldsymbol{g}_1^{row},$$

$$\vdots$$

$$\boldsymbol{s}_N \boldsymbol{G} = [g_{N1} \quad g_{N2} \quad \cdots \quad g_{NN}] = \boldsymbol{g}_N^{row} \quad (11)$$

where $\boldsymbol{g}_i^{row} (i = 1,...,N)$ is the row vector of $\boldsymbol{G}$.

Under these circumstances, $\boldsymbol{G}$ can be recovered correctly. However, the received signals at the eavesdroppers' sides are

$$\boldsymbol{y}_1 = \boldsymbol{h}_1 \otimes \boldsymbol{g}_1^{row} + \boldsymbol{n}_1, \ldots,$$

$$\vdots$$

$$\boldsymbol{y}_N = \boldsymbol{h}_N \otimes \boldsymbol{g}_N^{row} + \boldsymbol{n}_N \qquad (12)$$

In order to describe the randomness of fading coefficient and noise, we use subscript number to distinguish in e.g.(12).

In CPA, the eavesdroppers have a set of pairs $\{\boldsymbol{s}_i, \boldsymbol{y}_i\}$ .When transmitted over a Rayleigh fading channel and detected with an ideal phase coherent reference signal, the average symbol error probability(SEP) of M-PSK can be written as[25]

$$P_s(E) = \left(\frac{M-1}{M}\right)\left\{1 - \sqrt{\frac{g_{PSK}\bar{\gamma}_S}{1+g_{PSK}\bar{\gamma}_S}} \cdot \frac{M}{(M-1)\pi} \cdot \left[\frac{\pi}{2} + \tan^{-1}\left(\sqrt{\frac{g_{PSK}\bar{\gamma}_S}{1+g_{PSK}\bar{\gamma}_S}} \cot\frac{\pi}{M}\right)\right]\right\} \qquad (13)$$

where $g_{PSK} \triangleq \sin^2(\pi/M)$, $\bar{\gamma}_S$ is the average SNR per symbol.

Based on e.g.(12), $\boldsymbol{G}$ can be recovered as the probability

$$P_{correct} = \frac{(1 - P_S(E))^{N \times N}}{N_{\max} - 1} \qquad (14)$$

For QPSK

$$P_s(E) = \left(\frac{3}{4}\right)\left\{1 - \sqrt{\frac{\bar{\gamma}_S}{2+\bar{\gamma}_S}} \cdot \frac{4}{3\pi} \cdot \left[\frac{\pi}{2} + \tan^{-1}\left(\sqrt{\frac{\bar{\gamma}_S}{2+\bar{\gamma}_S}} \cot\frac{\pi}{4}\right)\right]\right\} \qquad (15)$$

$$P_{correct} = \frac{1}{N_{\max} - 1} \cdot \left(\frac{1}{4} + \frac{1}{\pi}\sqrt{\frac{\bar{\gamma}_S}{2+\bar{\gamma}_S}} \cdot \left[\frac{\pi}{2} + \tan^{-1}\left(\sqrt{\frac{\bar{\gamma}_S}{2+\bar{\gamma}_S}}\right)\right]\right)^{N \times N}$$

$$= \frac{1}{N_{\max} - 1} \cdot \left(\frac{1}{4} + \frac{1}{2}\sqrt{\frac{\bar{\gamma}_S}{2+\bar{\gamma}_S}} + \frac{1}{\pi}\sqrt{\frac{\bar{\gamma}_S}{2+\bar{\gamma}_S}} \cdot \tan^{-1}\left(\sqrt{\frac{\bar{\gamma}_S}{2+\bar{\gamma}_S}}\right)\right)^{N \times N} \qquad (16)$$

5.3 Known Plaintext Attacks (KPA)

Suppose that the eavesdropper knows a set of N information messages $\{\boldsymbol{s}_1,...,\boldsymbol{s}_N\}$ encrypted based on MPLE scheme and the associated received signals $\{\boldsymbol{y}_1,...,\boldsymbol{y}_N\}$. It is assumed that $\boldsymbol{s}_i' = \boldsymbol{s}_i\boldsymbol{G}$, e.g.(9) can be written as

$$\boldsymbol{y}_i = \boldsymbol{h}_i \odot \boldsymbol{s}_i' + \boldsymbol{n}_i \qquad (17)$$

Under these circumstances, the correct probability of $\boldsymbol{s}_i'(i = 1,2,...,N)$ is same as e.g.(14). Given $\boldsymbol{s}_i$ $(i = 1,2,...,N)$, $\boldsymbol{G}$ can be attained based on $\boldsymbol{s}_i'(i = 1,2,...,N)$ as follow

$$\boldsymbol{G} = \boldsymbol{S}^{-1} \times \boldsymbol{S}' \qquad (18)$$

where $\boldsymbol{S}$ and $\boldsymbol{S}'$ are matrixes based on $\boldsymbol{s}_i(i = 1,2,...,N)$ and $\boldsymbol{s}_i'(i = 1,2,...,N)$ respectively.

From the view of communication receiver, the correct probability of attack should written as

$$P_{correct}^{Modu} = P_{reco}(Modu) \cdot P_{correct} \qquad (19)$$

where $P_{reco}(Modu)$ is the correct probability of recognizing modulation $Modu$.

6. Performance Evaluations

In this section, we show simulation results about attack success probability and performance advantage of the MPLE scheme.

6.1 Attack success probability

From the view of communication receiver, the correct recognition of modulation is also an important part of attack success. In MPLE scheme, the modulation constellation is different from conventional modulation, which increase the security and decrease the attack success probability. Table 2 shows the correct recognition probability of MPLE scheme($N \geq 2$) considering conventional modulation set{BPSK, QPSK, 8PSK, 16QAM, 16APSK, 32APSK} at

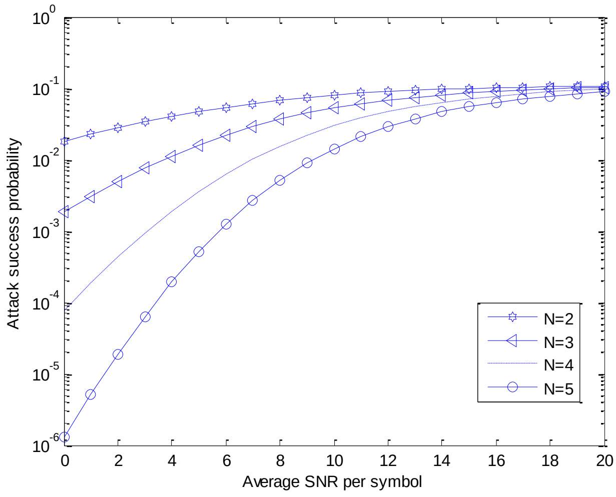
$SNR = 20dB$ for MPLE with QPSK.

Table 2 The correct recognition probability

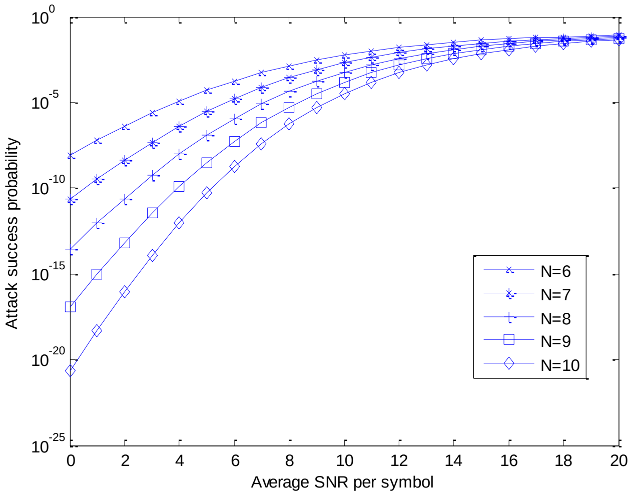
MPLE	Conventional modulations					
	BPSK	QPSK	8PSK	16QAM	16APSK	32APSK
QPSK, N=2	0	0.4%	0.1%	18.3%	1.2%	80%
QPSK, N=3	0	10.2%	12.6%	12%	24.7%	40.5%
QPSK, N=4	0	19.5%	44%	3.7%	22.3%	10.5%

For practicality, it is easy for unconventional modulation constellation to obfuscate the eavesdropper. Though the correct recognition probability is higher for larger N, the eavesdropper will choose the modulation with highest probability. Under the premise of wrong choice, the correct probability of recovering $\boldsymbol{G}$ is lower than that is in e.g.(14).

When QPSK and $N_{\max} = 10$ are assumed, attack success probability based on e.g.(14) is shown in Fig.7. Except for recognition probability, we only consider correctly recovering $\boldsymbol{G}$ here. Because of unknown N, the attack success probability is near $1/(N_{\max} - 1)$ gradually as $\bar{\gamma}_S$ increasing. However, attack success probability will be lower when the correct recognition probability is considered. Under the condition of $SNR = 20dB$ and $N = 2$, the attack success probability is lower than 10^{-3}.



(a)



(b)

Fig.7. *Attack success probability*
(a)N=2~5 **(b)**N=6~10

6.2 Performance advantage under fading channel

Generally, the BER performance lies in the physical-layer techniques, which has nothing to do with upper layer encryption algorithms. For legitimate receiver, the performance of the system with conventional encryption is same as the system without encryption.

In order to demonstrate the performance advantage of MPLE scheme, simulation is shown as follow, which is done between the same communication system with MPLE scheme and with the conventional encryption using higher layer cipher, such as AES, DES etc. In the simulation system, rate-1/3 convolutional code with generator polynomial G=[13 15 17] is used. The modulation is QPSK, $N = 3$ and frame length is 512. We assume the channel is Rayleigh fading channel, in which each symbol is i.i.d.

From Fig.8, it can be seen that our MPLE scheme can achieve better performance compared to the system with conventional encryption, where at BER of 10^{-5}, 1.7dB gain can be achieved. The performance advantage is derived from the diversity in our scheme.

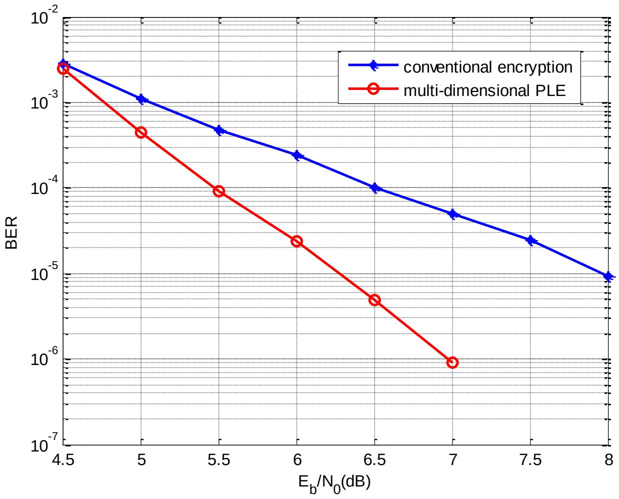


***Fig 8.** Performance of legitimate receiver with MPLE and conventional encryption*

For some PLE schemes, encrypted constellation is away from the optimal scheme because of phase rotation and amplitude changed, which lead to lower performance. The security is achieved by sacrificing the reliability. Such as the scheme based on random phase rotation in [9] , the gain is lost in both AWGN and quasi-static Rayleigh channel. A PLE method for OFDM/OQAM in[12] pay around 1~4 dB SNR penalty compared to no encryption. For the scheme in[26], the OSNR(optical signal-to-noise ratio) of the decrypted signal need 2.5 dB more than that of the original input 8PSK signal in order to achieve a BER lower than 10^{-3} . Compared with those PLE schemes, the performance advantage of our scheme is more obvious.

7. Conclusions

In order to cope with the security problem under fading channel, a novel MPLE scheme is proposed. The advantage of secrecy and reliability derives from the rotation and diversity gain of multi-dimensional constellation respectively. We discussed the encryption, the combined demodulation and decryption in detail. The security analysis emphasizes attack success probability of CPA and KPA. The simulation results about attack success probability and performance advantage shows that the MPLE scheme has the advantage on security and reliability under fading channel.

8. Acknowledgment

This work was supported in part by a grant from the National Natural Science Foundation of China under Grants No.61372098, No.61502518 and No.61702536.

9. References

[1]. Zuquete, A. and J. Barros. Physical-layer encryption with stream ciphers. IEEE International Symposium on Information Theory (ISIT), Toronto, Canada, July 6-11, 2008, pp. 106-110.

[2]. Ahmad, A., A. Biri and H. Afifi. Study of a new physical layer encryption concept. IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2008, pp. 860-865.

[3]. Kanter, G.S., D. Reilly and N. Smith, Practical physical-layer encryption: the marriage of optical noise with traditional cryptography. IEEE Communications Magazine, 2009. 47(11): p. 74-81.

[4]. Kanter, G.S., et al., Exploiting quantum and classical noise for securing high-speed optical communication networks . Proc. SPIE, vol.5842, pp. 74-86, May 2005.

[5]. Tahir, M., S.P.W. Jarot and M.U. Siddiqi. Wireless physical layer security using encryption and channel pre-compensation. in International Conference on Computer Applications and Industrial Electronics (ICCAIE), December 5-7, 2010, Kuala Lumpur, Malaysia, pp. 304-309.

[6]. Bi, S., X. Yuan and Y. Jun, Pragmatic Physical Layer Encryption for Achieving Perfect Secrecy. arXiv preprint arXiv:1210.5599, 2012.

[7]. Bi, S., X. Yuan and Y.J. Zhang. DFT-based physical layer encryption for achieving perfect secrecy. IEEE International Conference on Communications (ICC), 2013, pp.2211-2216.

[8]. Huo, F. and G. Gong, XOR encryption

versus phase encryption, an in-depth analysis. IEEE Trans. Electromagnetic Compatibility, vol.57, no.4, pp. 903-911, Jan 2015.

[9]. Xu, Z., et al. Achieving secure communication through random phase rotation technique. in Wireless Communications and Mobile Computing Conference. IEEE Wireless Communications and Mobile Computing Conference, pp.2073-2078. 2017

[10]. Gao, B., et al., A Hiding Algorithm for OFDM Constellation Mapping Based on Wireless Physical Layer Encryption. Journal of Applied Sciences, vol.13, no.18, pp.3790-3797, 2013.

[11]. Gao, B., et al. New physical layer encryption algorithm based on DFT-S-OFDM system. in Mechatronic Sciences, Electric Engineering and Computer (MEC), Shenyang, China, Dec 20-22, 2013, pp.2018-2022.

[12]. Sakai, M., H. Lin and K. Yamashita, Intrinsic Interference Based Physical Layer Encryption for OFDM/OQAM. IEEE Communications Letters, 2017. PP(99): p. 1-1.

[13]. Chorti, A. Masked-OFDM: A physical layer encryption for future OFDM applications. in IEEE Global Telecomm. Conf. (GLOBECOM), 2010, pp.1254-1258.

[14]. Huo, F. and G. Gong. A new efficient physical layer OFDM encryption scheme. IEEE International Conference on Computer Communications (INFOCOM), 2014, pp.1024-1032.

[15]. Tollefson, E., B.R. Jordan and J.D. Gaeddert. Out-phased array linearized signaling (OPALS): A practical approach to physical layer encryption. in Military Communications Conference (Milcom), 2015, pp. 294-299.

[16]. Boutros, J. and E. Viterbo, Signal space diversity: a power- and bandwidth-efficient diversity technique for the Rayleigh fading channel. IEEE Transactions on Information Theory, 2010. 44(4): p. 1453-1467.

[17]. Tran, N.H., H.H. Nguyen and T. Le-Ngoc. Application of signal space diversity over multiplicative fading channels. IEEE Signal Processing Lett., vol.16, no.3, pp.204-207, March 2009.

[18]. Tran, N.H., H.H. Nguyen and T. Le-Ngoc, BICM-ID with Signal Space Diversity over Cascaded Rayleigh Fading Channels. IEEE Transactions on Communications, 2008. 56(10): p. 1561 - 1568.

[19]. Tran, N.H., H.H. Nguyen and T. Le-Ngoc, Performance Analysis and Design Criteria of BICM-ID with Signal Space Diversity for Keyhole Nakagami- Fading Channels. IEEE Transactions on Information Theory, 2009. 55(4): p. 1592-1602.

[20]. Tran, N.H., H.H. Nguyen and T. Le-Ngoc, Performance of BICM-ID with Signal Space Diversity. Wireless Communications IEEE Transactions on, 2006. 6(5): pp.1732-1742.

[21]. Li, X., A. Chindapol and J.A. Ritcey, Bit-interleaved coded modulation with iterative decoding and 8 PSK signaling. Communications IEEE Transactions on, 2002. 50(8): p. 1250-1257.

[22]. Tran, N.H. and H.H. Nguyen, Design and performance of BICM-ID systems with hypercube constellation. IEEE Transactions on Wireless Communications, 2006. 5(5): p. 1169-1179.

[23]. Huang, Y. and J. Lei, Research on recognition of modulation signals in satellite communication. Systems Engineering & Electronics, 2009. 31(6): p. 1303-1306.

[24]. Swami, A. and B.M. Sadler, Hierarchical Digital Modulation Classification Using Cumulants. IEEE Transactions on Communications, 2000. 48(3): p. 416-429.

[25]. Simon, M.K. and M.S. Alouini. Digital Communication Over Fading Channels: A Unified Approach to Performance Analysis. Wiley-IEEE Press, 2000.

[26]. Zhang, M., et al., Optical encryption/decryption of 8PSK signal using FWM-based modified XOR. Applied Optics, 2015. 54(25): p. 7813.