A New Efficient Physical Layer OFDM Encryption Scheme

Fei Huo
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Canada
Email: fhuo@uwaterloo.ca

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Canada
Email: ggong@uwaterloo.ca

***Abstract*—In this paper, we propose a new encryption scheme for OFDM systems. The reason for physical layer approach is that it has the least impact on the system and is the fastest among all layers. This scheme is computationally secure against the adversary. It requires less key streams compared with other approaches. The idea comes from the importance of orthogonality in OFDM symbols. Destroying the orthogonality create intercarrier interferences. This in turn cause higher bit and symbol decoding error rate. The encryption is performed on the time domain OFDM symbols, which is equivalent to performing nonlinear masking in the frequency domain. Various attacks are explored in this paper. These include known plaintext and ciphertext attack, frequency domain attack, time domain attack, statistical attack and random guessing attack. We show our scheme is resistant against these attacks. Finally, simulations are conducted to compare the new scheme with the conventional cipher encryption.**

I. Introduction

OFDM was first proposed by Chang [4]. It is a multiplexing method in which data are transmitted over the equally spaced, overlapped carrier frequencies. Advantages of OFDM include: 1) It has high spectral efficiency and can support various underlying modulation schemes such as PSK, QAM to achieve high data rate; 2) It can resist against ISI as a result of longer symbol time and artificially introduced CP. The modulation and demodulation of OFDM signals can be implemented in hardware efficiently using Inverse Fast Fourier Transform (IFFT) and Fast Fourier Transform (FFT) respectively. Consequently, OFDM has been adopted in many standards. This include next generation mobile technologies 3GPP LTE [2], IEEE 802.16 WiMax [10], digital audio broadcasting (DAB) [7] and digital video broadcasting (DVB) [8].

On the other hand, the secrecy of messages has become increasingly more important in the past decade. Almost all standards have incorporated security algorithms to ensure that data has been securely transmitted over the channel. For instance, LTE have stream ciphers SNOW 3G, ZUC and block cipher AES [1]. GSM have adopted stream cipher A5 [5], etc.

To ensure the secrecy of messages is not revealed to unwanted parties, various encryptions mechanisms are usually applied to the messages before they are transmitted. In the conventional cipher encryption for in wireless communications, each message bit is independently encrypted with a key stream bit through XOR operation to produce one ciphertext bit. At the receiver, the same XOR operation between the ciphertext bit and the key stream bit is performed to recover the message. In this approach, to produce one bit of ciphertext requires one bit of key stream. This could be problematic in a high speed data transmission application with constrained devices. For instance, 3GPP LTE standard has been designed to meet a downlink (DL) peak data rate of 300 Mb/s [3]. Consequently, the key streams generation rate has to be the same to achieve the maximum security. Assuming the encryption cipher is AES [15] used in counter mode, to the best of authors' knowledge, although the rate can vary from 2.56 Gb/s to 62.6 Gb/s depending on the implementations, this require a hardware of 34.5 Kgates and 979.3 Kgates respectively [19]. It is impractical with constrained devices such as mobiles. The smallest AES implementation requires 2.4 Kgates, but it can only generate key streams at a rate of 57 Kb/s [13]. This does not nearly meet the requirement set forth by LTE.

Phase encryption was first introduced in optical encryptions. It is a promising technique that takes advantage of high resolution optical materials [9]. In the field of electronic ciphering, various encryption techniques for OFDM systems have also been proposed, such as chaos based constellation scrambling [11], masked approach [6] and noise enhance approach [18]. None of these techniques would solve the problem described above. In [18], authors have proposed the use of 8-bit key streams to encrypt one time domain OFDM sample. However, no analysis was given in the paper.

In this paper, we investigate how we could more efficiently encrypt the data while still achieving the acceptable level of security. Our contributions are summarized below:

- We propose a new physical layer encryption scheme for OFDM systems which we called *OFDM Enc*. The reason for physical layer approach is that it has the least impact on the system and it is the fastest among all layers. This scheme is computationally secure against the adversary. The encryption is performed by changing the sign (phase)

978-1-4799-3360-0/14/$31.00

of the time domain OFDM samples. This is equivalent to performing a nonlinear masking on the frequency information symbols.
- An initial investigation on the encryption efficiency and security of this new scheme is evaluated. Various attacks were explored. These include known plaintext and ciphertext attack, frequency domain attack, time domain attack, statistical attack and random guessing.
- Simulations were performed to compare the performance in terms of symbol error rate (SER) of *OFDM Enc* with the conventional cipher encryption.

The rest of this paper is organized as follows. In Section II, we introduce the necessary notations, system and adversarial models used in the paper. We also give some background on the OFDM system, conventional cipher encryptions and decryptions. In Section III, we present our scheme *OFDM Enc* along with some of its properties. In Section IV, we perform a thorough security analysis on our proposed scheme. In Section V, we present simulation results on our scheme compared with the conventional cipher encryption. Section VI concludes our paper and lists some future research directions.

II. Prelimenaries and Background

A. Prelimenaries

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

- $D_{\mathbf{z}}$ is a diagonal matrix with the elements $\{z_0, \cdots, z_{N-1}\}$ and dimension N.
- Let F and F^{-1} denote the DFT and IDFT matrix respectively.
- We use bold letters to denote vectors of length N. i.e., $\mathbf{M} = (M_0, \cdots, M_{N-1})$.
- We use capital letters and lowercase letters to represent frequency and time domain symbols respectively.
- For two vectors, $\mathbf{w} = (w_0, \cdots, w_{N-1})$ and $\mathbf{z} = (z_0, \cdots, z_{N-1})$, the term-wise product of $\mathbf{w}$ and $\mathbf{z}$ is denoted as $\mathbf{w} \cdot \mathbf{z} = (w_0 z_0, w_1 z_1, \cdots, w_{N-1} z_{N-1})$.
- We denote $\mathbf{w}^T$ to be the transpose of $\mathbf{w}$.
- We define keys to be seeds assigned to the user which are loaded into the stream cipher to generate the key streams. Key streams are used for encryption.

B. Background

1) OFDM System: The baseband OFDM transmitter is drawn in Figure 1. Note here we omit data preprocessing blocks such as channel codings and source codings. The frequency domain symbols $\mathbf{M} = (M_0, M_1, \cdots, M_{N-1}) \in \mathbb{C}^N$ are modulated symbols to be transmitted. The number of values M_k can take is 2^r, where r is number of bits per symbol and it will depend on the underlying modulation scheme. i.e., $r = 2$ for QPSK and $r = 4$ for 16-QAM. Their corresponding baseband time domain OFDM symbol $\mathbf{m} = (m_0, m_2, \cdots, m_{N-1})$ obtained by performing inverse discrete Fourier transform (IDFT) on $\mathbf{M}$ is as follows:

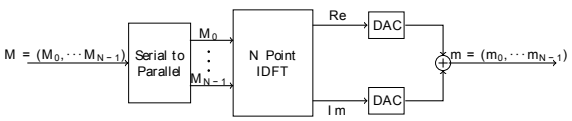

Fig. 1. Baseband OFDM transmitter

$$m_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} M_k e^{\frac{j2\pi ik}{N}}, \quad i, k = 0, 1, \cdots, N-1. \tag{1}$$

where $i = 0, 1, \cdots N-1$. In general, m_i is complex valued.

The baseband OFDM receiver is shown in Figure 2. During the demodulation, assuming the environment to be noiseless, symbols transmitted over different frequencies are orthogonal, hence they will not interfere with each other. By simply applying the discrete Fourier transform (DFT), correct modulated symbols can be recovered. This is shown as follows:

$$M_k = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} m_i e^{-\frac{j2\pi ik}{N}}, \quad i, k = 0, 1, \cdots, N-1. \tag{2}$$

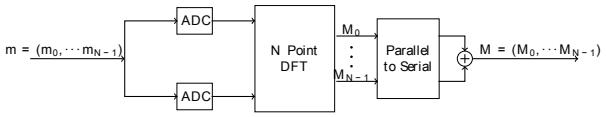

Fig. 2. Baseband OFDM Receiver

2) Conventional Cipher Encryption: For conventional cipher encryption, the baseband OFDM transmitter is shown in Figure 3. Key streams $\mathbf{K}$ are first bitwise XORed with messages $\mathbf{S}$ to produce ciphertext $\mathbf{C}$. Then subcarrier mapping will now map ciphertext instead of messages into modulated symbols. Finally, IDFT of modulated ciphertext will be applied to obtain the encrypted OFDM symbols. Note that this encryption scheme is generic and works for any communication systems not just OFDM. At the receiver, the reverse procedures are performed to correctly recover the message.

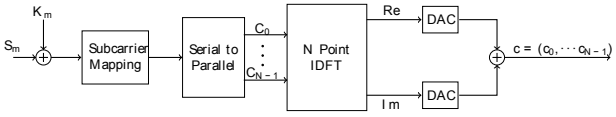

Fig. 3. Conventional Stream Cipher Encryption

3) System Assumption: We assume two pseudorandom sequence generators (PRSG) are available to produce two key streams **a** and **b** where a_i and $b_i \in \{-1, 1\}$. Alternatively, one can also use one PRSG and divide into two key streams.

4) Adversarial Model: We assume the adversary has the complete knowledge of the channel and protocols used for transmission. He can intercept all messages exchanged between the transmitter and the receiver. From this, he can use various techniques to try to recover the key, key streams and/or messages. We do not consider the scenario where the adversary can exploit the weaknesses in the cipher to recover keys and/or key streams, we assume the cipher is perfectly secure.

III. OFDM ENC SCHEME

OFDM Enc is drawn from the idea that OFDM symbols are sensitive to phase noise [14]. The encryption is performed by varying the sign (phase) of each of in-phase and quadrature component of time domain OFDM samples according to two binary key streams, thereby destroying the orthogonality of OFDM symbols. Without the knowledge of these two key streams, the adversary will have a high error probability when he tries to decode.

A. Encryption and Decryption of OFDM Enc

a) Encryption: The transmitted N-point time domain OFDM symbol after the encryption can be represented as follows:

$$c_i = Re\{\sum_{k=0}^{N-1} M_k e^{\frac{j2\pi ik}{N}}\} \times a_i + jIm\{\sum_{k=0}^{N-1} M_k e^{\frac{j2\pi ik}{N}}\} \times b_i, \quad (3)$$

where $i, k = 0, 1, \cdots, N-1$. This is shown in Figure 4.

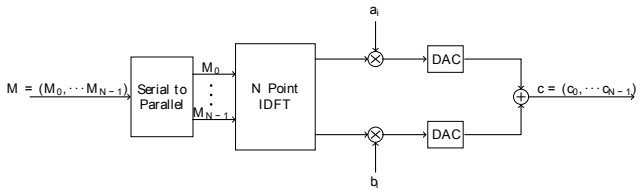

Fig. 4. *OFDM Enc* Encryption

This is equivalent to having two pseudo-random sequences **a** and **b** acting on the real and imaginary part of time domain data symbols m_i from (1):

$$c_i = Re\{m_i\} \times a_i + jIm\{m_i\} \times b_i. \quad (4)$$

b) Decryption: For an intended OFDM receiver, after the analogue-to-digital convertor (ADC), the receiver recovers the signal $\mathbf{c} = (c_0, \cdots, c_{N-1})$, which is the ciphertext produced in (4). The receiver first locally generates two pseudorandom sequences $\mathbf{a}$ and $\mathbf{b}$, then he computes

$$Re(m_i) = a_i Re(c_i) \text{ and } Im(m_i) = b_i Im(c_i). \quad (5)$$

This is shown in Figure 5. After recovering **m**, it follows the standard OFDM receiver structure, the information bits are reconstructed.

For the adversary, since he does not share the key streams with the transmitter, he cannot generate the pseudorandom sequences **a** and **b**. Consequently, the adversary cannot perform the operations in (5).

The key difference between *OFDM Enc* and the conventional cipher encryption lies in when the data are being encrypted. In the conventional encryption, data are encrypted by bitwise XOR operations in the frequency domain before the IDFT block. In *OFDM Enc*, encryption is performed by term-wise multiplication in the time domain after the IDFT block. We use the following example to illustrate the encryption and decryption process of *OFDM Enc*.

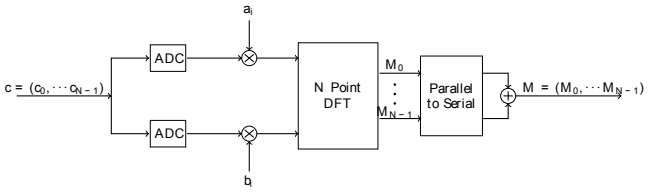

Fig. 5. *OFDM Enc* Decryption

c) Example 1: Assume $N = 16$ and the modulation scheme is QPSK. This implies OFDM symbols are composed of 16 QPSK modulated subcarriers. Let **S** be information symbols composed of 2 bits, **M** be modulated QPSK symbols, **a** and **b** be two key streams. These data parameters are shown in Table I.

TABLE I
DATA PARAMETERS, OFDM SYMBOLS AND ENCRYPTED OFDM SYMBOLS

S	M	a	b	m	c
3	$1-j$	-1	-1	$-0.250+0.125j$	$0.250-0.125j$
0	$-1+j$	1	1	$0.469-0.298j$	$0.469-0.298j$
3	$1-j$	-1	1	$0.037-0.037j$	$-0.037-0.037j$
1	$-1-j$	-1	1	$-0.144-0.115j$	$0.144-0.115j$
0	$-1+j$	1	1	$-0.125+0.250j$	$-0.125+0.250j$
1	$-1-j$	-1	-1	$-0.401-0.365j$	$0.401+0.365j$
1	$-1-j$	-1	1	$-0.140-0.037j$	$0.140-0.037j$
1	$-1-j$	-1	-1	$0.306-0.048j$	$-0.306+0.048j$
2	$1+j$	1	1	$0.500+0.125j$	$0.500+0.125j$
2	$1+j$	-1	1	$0.238-0.202j$	$-0.238-0.202j$
0	$-1+j$	-1	-1	$0.213-0.213j$	$-0.213+0.213j$
0	$-1+j$	-1	-1	$0.144+0.115j$	$-0.144-0.115j$
2	$1+j$	1	-1	0.375	0.375
0	$-1+j$	-1	-1	$-0.306-0.135j$	$0.306+0.135j$
2	$1+j$	-1	-1	$0.390-0.213j$	$-0.390+0.213j$
1	$-1-j$	-1	-1	$-0.346+0.048j$	$0.346-0.048j$

Encryption: We know

$$c_i = Re\{m_i\} \times a_i + jIm\{m_i\} \times b_i, 0 \le i \le 15$$

After computing 16-point FFT, we have **m** and **c** respectively in Table I.

Decryption: We will explore the decryption performed by both the legitimate receiver and the adversary. Since the adversary does not have the key streams, we assume his strategy is to follow standard OFDM demodulation procedure on the ciphertext. We denote **M** and **S** to be the demodulated and decoded symbol obtained by the legitimate receiver, $\mathbf{M}'$ and $\mathbf{S}'$ to be the demodulated and decoded symbol obtained by the adversary respectively. The result is shown in Table II. We observe in this particular example, the adversary's decoding SER is $\frac{13}{16}$ or 81.25%.

B. Compressed Key Stream Length

If M_k is a 2^r-ary modulated symbol, in the conventional cipher encryption, this would require r-bit key streams to

TABLE II
DECODED MESSAGES BETWEEN THE LEGITIMATE RECEIVER AND THE ADVERSARY

M	**S**	**M′**	**S′**
$1-j$	3	$1.438+0.373j$	2
$-1+j$	0	$0.977-0.875j$	3
$1-j$	3	$-0.707-0.457j$	1
$-1-j$	1	$-0.333-0.977j$	1
$-1+j$	0	$1.731-1.042j$	3
$-1-j$	1	$0.156-0.743j$	2
$-1-j$	1	$-0.034+0.631j$	0
$-1-j$	1	$-1.550-0.344j$	1
$1+j$	2	$-0.438+0.835j$	0
$1+j$	2	$-2.184+0.374j$	0
$-1+j$	0	$1.707-0.043j$	3
$-1+j$	0	$-0.874-1.524j$	1
$1+j$	2	$1.269+0.835j$	2
$-1+j$	0	$1.051+0.757j$	2
$1+j$	2	$1.034-1.131j$	3
$-1-j$	1	$0.757-0.156j$	3

generate r-bit ciphertext. In *OFDM Enc*, even though M_k carries r bits plaintext, it will be encrypted by 2 bits key streams for any r. We define the efficiency of encryption ϵ as a measurement for key streams required between conventional cipher encryption scheme and *OFDM Enc*:

$$\epsilon = \frac{r}{2} \tag{6}$$

For $r \geq 2$, ϵ is greater than one, which indicates that key streams required are less using *OFDM Enc*. Even for the worst case of QPSK where $r = 2$, the key streams required for both encryption schemes are identical. The increased efficiency of *OFDM Enc* may prove to be beneficial in constrained devices and high speed applications.

C. Maintained PMEPR

One major drawback of OFDM is the peak-to-mean envelope power ratio (PMEPR) [12]. This is a measurement of peak signal power to the average power. In the case when all subcarriers add up constructively, PMEPR can be as high as N. This may drive the power amplifier into the non-linear region, potentially damaging the power amplifier and/or introducing non-linear distortions. In *OFDM Enc*, by only changing the signs of time domain signals, the magnitude of the transmitted of the encrypted and the original OFDM samples remain unchanged. i.e., $|c_i| = |m_i|$, for $0 \leq i < N$. Thus, the PMEPR of transmitted encrypted OFDM symbols remain unaffected.

If the OFDM symbols are precoded to ensure certain PMEPR levels, then by adopting *OFDM Enc*, the PMEPR of encrypted OFDM symbols is maintained. Note that the aforementioned schemes [11], [6] would not achieve this. PMEPR of encrypted OFDM symbols will inevitably be different and even unpredictable from un-encrypted OFDM symbols.

IV. SECURITY ANALYSIS

In this section, we present security analysis on our proposed scheme. More specifically, we consider 5 different attacks. They are plaintext and ciphertext attack, frequency domain attack, time domain attack, statistical attack and random guessing attack. We show *OFDM Enc* is resilient against all these attacks.

A. Known Plaintext and Ciphertext Attacks

If the adversary knows modulated symbols **M**, then he can compute the OFDM symbol **m**. From (5), both a_i and b_i can be recovered. Therefore, he can recover the key streams **a** and **b**. This is the same attack as the conventional cipher encryption.

On the other hand, if the adversary only knows a subset of messages $\{M_0, M_1, \cdots, M_{N-1}\}$, he cannot obtain all the correct time domain symbols. As a result, he can statistically estimate **a** and **b**, but he is not guaranteed to recover any key streams with 100% certainty. More discussion on the recovery of messages given a subset of keys are comprised will be discussed in the next section. Given a subset of key streams to find messages are essentially equivalent to given a subset of messages to find key streams. In this case, *OFDM Enc* is more resistant against known plaintext and ciphertext attack.

B. Frequency Domain Attack

In this subsection, we explore the possibility of launching the attack in the frequency domain. The adversary may attempt to directly apply the DFT F on **c** as follows and then perform the decoding:

$$F\mathbf{c}^T = F\{(\mathbf{a} \cdot Re(\mathbf{m}))^T + j(\mathbf{b} \cdot Im(\mathbf{m}))^T\}. \tag{7}$$

We will try to express the above equation in the matrix format. Before this, we first take a look at the scenario where no encryption was present. Then we will compare the demodulation of unscripted messages with ciphertext from (7). From (1), if we write M_k in terms of real part X_k and imaginary part Y_k and $e^{\frac{j2\pi ik}{N}}$ in terms of $\cos(2\pi ik/N)+j\sin(2\pi ik/N)$ we have

$$m_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \{(X_k + jY_k)(\cos(ik\theta_N) + j\sin(ik\theta_N))\},$$

where $\theta_N = \frac{2\pi}{N}$.

This gives

$$Re(m_i) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (X_k \cos(\theta_N ik) - Y_k \sin(\theta_N ik)) \tag{8}$$

$$Im(m_i) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (X_k \sin(\theta_N ik) + Y_k \cos(\theta_N ik)) \tag{9}$$

Thus we have the matrix representation of (1) as follows:

$$\mathbf{m}^T = F^{-1}\mathbf{M}^T \tag{10}$$

where F^{-1} is an N by N matrix given by:

$$F^{-1} = \frac{1}{\sqrt{N}}(f_{ik})_{N\times N} \tag{11}$$

and $f_{ik} = e^{jik\theta_N}, 0 \le i,k < N$. Writing $\mathbf{m}$ in terms of real part and imaginary part of $\mathbf{M}$, (10) becomes

$$\begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ \vdots \\ m_{N-1} \end{pmatrix} = F_{\cos}^{-1} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{pmatrix} - F_{\sin}^{-1} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_{N-1} \end{pmatrix} + jF_{\sin}^{-1} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{pmatrix} + jF_{\cos}^{-1} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_{N-1} \end{pmatrix} \quad (12)$$

where

$$F_{\cos}^{-1} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \cos(\theta_N) & \cdots & \cos((N-1)\theta_N) \\ 1 & \cos(2\theta_N) & \cdots & \cos(2(N-1)\theta_N) \\ \vdots & \vdots & & \vdots \\ 1 & \cos(i\theta_N) & \cdots & \cos((N-1)i\theta_N) \\ \vdots & \vdots & & \vdots \\ 1 & \cos((N-1)\theta_N) & \cdots & \cos((N-1)^2\theta_N) \end{pmatrix} \quad (13)$$

and

$$F_{\sin}^{-1} = \frac{1}{\sqrt{N}} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & \sin(\theta_N) & \cdots & \sin((N-1)\theta_N) \\ 0 & \sin(2\theta_N) & \cdots & \sin(2(N-1)\theta_N) \\ \vdots & \vdots & & \vdots \\ 0 & \sin(i\theta_N) & \cdots & \sin((N-1)i\theta_N) \\ \vdots & \vdots & & \vdots \\ 0 & \sin((N-1)\theta_N)) & \cdots & \sin((N-1)^2\theta_N) \end{pmatrix} \quad (14)$$

Thus, the time domain OFDM symbol in (1) can be rewritten in matrix format in cosine and sine representations as follows:

$$\mathbf{m}^T = (F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) + j(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T). \quad (15)$$

If no encryption is present, the receiver simply computes the DFT of received signal $\mathbf{m}$ to recover the message $\mathbf{M}$:

$$\begin{aligned} \mathbf{M}^T &= F\mathbf{m}^T \\ &= (F_{\cos} + jF_{\sin})((F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) + j(F_{\sin}^{-1}\mathbf{X}^T \\ &\quad + F_{\cos}^{-1}\mathbf{Y}^T)) \\ &= (F_{\cos}(F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) - F_{\sin}(F_{\sin}^{-1}\mathbf{X}^T + \\ &\quad F_{\cos}^{-1}\mathbf{Y}^T)) + j(F_{\cos}(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T)) + \\ &\quad F_{\sin}((F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T)). \end{aligned}$$

where $F = (f_{ik}^{-1})_{N\times N}$ is an $N \times N$ matrix. Moreover, we know $F_{\cos} = (\cos(ik\theta_N))_{0\le i,k<N} = F_{\cos}^{-1}$, and $F_{\sin} = (\sin(-ik\theta_N))_{0\le i,k<N} = -F_{\sin}^{-1}$, they are also $N \times N$ matrices. We can simplify the above equations as follows:

$$\begin{aligned} \mathbf{M}^T &= (F_{\cos}^2\mathbf{X}^T + F_{\cos}F_{\sin}\mathbf{Y}^T + F_{\sin}^2\mathbf{X}^T - F_{\sin}F_{\cos}\mathbf{Y}^T) \\ &\quad + j(F_{\sin}F_{\cos}\mathbf{X}^T + F_{\sin}^2\mathbf{Y}^T - F_{\cos}F_{\sin}\mathbf{X}^T + \\ &\quad F_{\cos}^2\mathbf{Y}^T) \quad (16) \\ &= (F_{\cos}^2 + F_{\sin}^2)\mathbf{X}^T + j(F_{\sin}^2 + F_{\cos}^2)\mathbf{Y}^T \\ &= \mathbf{X}^T + j\mathbf{Y}^T. \end{aligned}$$

The multiplication between matrices $F_{\cos}F_{\sin} = 0_{N\times N}$. This is described in the following proposition. The proof is omitted due to space limitations.

Proposition 1: For two $N \times N$ matrices defined by $F_{\cos} = (\cos(ik\theta_N))_{0\le i,k<N}$ and $F_{\sin} = (\sin(-jk\theta_N))_{0\le j,k<N}$, their product $F_{\cos}F_{\sin}$ is an $N \times N$ zero matrix. i.e., $F_{\cos}F_{\sin} = 0_{N\times N}$.

Consequently, we say $F_{\cos}$ to be orthogonal to $F_{\sin}$. Moreover, $F_{\cos}^2 + F_{\sin}^2 = I$, where I is an $N \times N$ identity matrix. Therefore, at the end of the DFT, receivers can correctly reconstruct message symbols $\mathbf{M}$ assuming the environment is noiseless.

Now examine the scenario where encryption has applied to the time domain OFDM symbols. The encrypted OFDM symbol defined in (4) is given in matrix form by

$$\mathbf{c}^T = D_{\mathbf{a}}(F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) + jD_{\mathbf{b}}(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T), \quad (17)$$

where $D_{\mathbf{a}}$ and $D_{\mathbf{b}}$ are diagonal matrices with elements $\{a_0, a_1, \cdots, a_{N-1}\}$ and $\{b_0, b_1, \cdots, b_{N-1}\}$ respectively.

If the adversary still directly takes the Fourier transform of $\mathbf{c}$, he can obtain the following result:

$$\begin{aligned} F\mathbf{c}^T &= F_{\cos}\mathbf{c}^T + jF_{\sin}\mathbf{c}^T \\ &= (F_{\cos}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T + F_{\cos}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T + \\ &\quad F_{\sin}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T - F_{\sin}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T) + \\ &\quad j(F_{\sin}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T + F_{\sin}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T - \\ &\quad F_{\cos}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T + F_{\cos}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T. \quad (18) \end{aligned}$$

Here, we clearly see the differences between un-encrypted messages and encrypted messages in the view of the adversary by comparing (16) and (18). There will be two types of distortions introduced. First, two matrices $F_{\cos}$ and $F_{\sin}$ are multiplied by another matrix $D_{\mathbf{a}}$ in between, which means their product is not 0 so they are no longer orthogonal. Second, $F_{\cos}D_{\mathbf{a}}F_{\cos} + F_{\sin}D_{\mathbf{b}}F_{\sin}$ and $F_{\cos}D_{\mathbf{b}}F_{\cos} + F_{\sin}D_{\mathbf{a}}F_{\sin}$ are longer adding up to a identity matrix as they do in (16). Consequently, for the adversary, by simply applying the standard demodulation procedure on the encrypted signals, he will demodulate the real part and imaginary part of time domain symbols into $\mathbf{X}'$ and $\mathbf{Y}'$ frequency domain signals as:

$$\begin{aligned} \mathbf{X}' &= F_{\cos}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T + F_{\sin}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T + \\ &\quad F_{\cos}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T - F_{\sin}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T \quad (19) \\ \mathbf{Y}' &= F_{\sin}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T - F_{\cos}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T + \\ &\quad F_{\sin}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T + F_{\cos}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T \quad (20) \end{aligned}$$

Note that these two types of decoding distortions are all non-linear from the frequency domain perspective. The encrypted OFDM symbols by *OFDM Enc* is equivalent to non-linear masking when viewed in the frequency domain.

The optimal detector should satisfy maximum a posterior probability (MAP) conditions. If each symbol is transmitted with equal probability, MAP decision rule is equivalent to maximum likelihood (ML) decoding. Moreover, if the channel is corrupted by additive white Gaussian noise (AWGN), then the optimal detector would become the minimum distance decoder [17]. Assuming this is the case, it is shown later in the simulations that without the knowledge of **a** and **b**, these distortions will cause the decoded symbols fall randomly among the different decision regions. Thus, the correct decoding probability P_c is same as random guessing at:

$$P_c = \frac{1}{2^r},$$

where 2^r is the underlying modulation rate.

C. Time Domain Attack

If $i = 0$, the real and imaginary portions of the OFDM symbol from (8) and (9) respectively become:

$$Re(m_0) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_k, \quad (21)$$

$$Im(m_0) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} Y_k. \quad (22)$$

If QPSK modulation is employed where $X_k, Y_k \in \{1, -1\}$, because we know the total number of subcarriers is N, we have also known the difference between transmitted 1's and -1's in $\mathbf{X}$ and $\mathbf{Y}$ is $Re(m_0)$ and $Im(m_0)$ respectively. Consequently, the adversary can recover exactly number of 1's and -1's in the message blocks. The searching complexity C to recover the $2N$ bits message block now becomes:

$$C = \binom{N}{m} \times \binom{N}{n}, \quad (23)$$

where m and n are respectively the number of 1's transmitted in the real and imaginary part of m_0.

This is not an immediate threat to this scheme. In a system where $N = 128$, which is the minimum FFT size in LTE [3], it can be shown that as long as number of 1's or -1's exceed 15 for each of real and imaginary block, the searching complexity to correctly recover $\mathbf{M}$ would exceed 2^{128}. Using elementary probability, in a message block of 128 bits, the probability it contains less than only 16 1's or -1's is less than 8.930×10^{-20}.

In the case of higher rate modulation schemes where $r > 2$, this attack becomes even more difficult as more combinations of $\mathbf{X}$ and $\mathbf{Y}$ would satisfy (21) and (22).

D. Statistical Attack

The adversary may exploit the statistical change in the encrypted OFDM symbols in order to launch an attack. It is well known that if the input data symbols are statistically independent, identically distributed and the number of sub-carriers N is large, then each OFDM sample m_i after IDFT block is independent Gaussian variables [16]. In fact, when $N = 64$, experiment results have already shown this is the case [16]. In LTE specifications, the minimum FFT size $N = 128$, therefore, it is reasonable to treat each time domain OFDM sample as an independent Gaussian random variables.

In this case, if each bit in the two key streams is uniformly distributed in $\{-1, 1\}$ and key streams are independent of information bits, these two should be valid and realistic assumptions, then by potentially changing the the sign of each of in-phase and quadrature component of time domain OFDM samples m_i, each encrypted sample c_i for $0 \leq i < N$ is also independent and identically distributed with the same mean and variance. This is due to Gausstian distribution is symmetrical along the vertical axis. The formal proof is omitted due to space limitation. The statistical distribution of the encrypted OFDM samples are identical to the original samples. Consequently, the adversary cannot exploit the statistical change of the signal due to encryption to launch an attack.

E. Random Guessing of OFDM Symbols

We assume that both the conventional cipher encryption and *OFDM Enc* use the same PRSG. The number of key streams required for encryption is rN in the conventional scheme and $2N$ in *OFDM Enc*. If the adversary randomly guess the key streams, then the successful probabilities of conventional scheme, denoted as $P_{succ,C-Enc}$ and *OFDM Enc* denoted as $P_{succ,OFDM-Enc}$, are given by

$$P_{succ,C-Enc} = 2^{-rN} \text{and } P_{succ,OFDM-Enc} = 2^{-2N}.$$

In this case, the conventional scheme is more resistant to random guessing for $r > 2$. This is because conventional scheme utilizes more key streams than *OFDM Enc*. However, for $N > 64$,

$$P_{succ,OFDM-Enc} = 2^{-2N} < 2^{-128}.$$

The smallest FFT size in LTE is $N = 128$. Thus, this attack of directly random guessing of the key stream bits is not a threat to those real systems.

V. Simulation Results

In this section, we have conducted three simulations in MATLAB to demonstrate the performance of *OFDM Enc* compared to the conventional cipher encryption. The cipher used is AES in counter mode which is the EEA2 confidentiality algorithm incorporated in LTE [1]. The odd bit key streams are used for encrypting real portion of the OFDM samples. The even bit key streams are used for encrypting imaginary portion of the OFDM samples. All simulation results are averaged over 10^5 OFDM symbols. Throughout all simulations, we assume the adversary tries to recover the message by directly

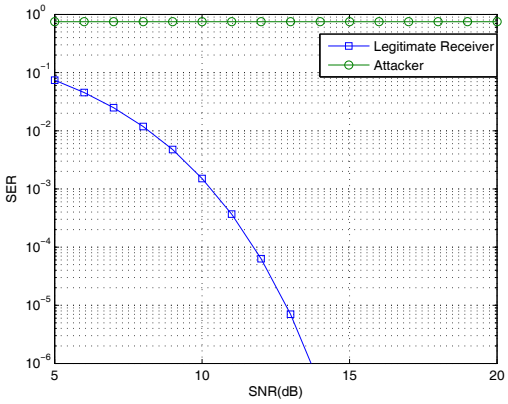

Fig. 6. Performance of Legitimate Receiver and Adversary under Different Noise Level with QPSK Modulation

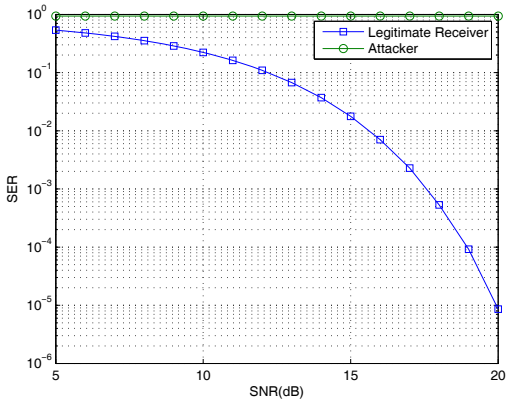

Fig. 7. Performance of Legitimate Receiver and Adversary under Different Noise Level with 16-QAM Modulation

applying the DFT on the encrypted OFDM symbols and then perform the decoding. Finally, we assume the channel is AWGN channel.

A. Simulation 1: Performance Evaluations under Different Noise Levels

The first simulation we conducted was to test the performance of our scheme under various noise level settings compared to a legitimate receiver. We simulated this with QPSK and 16-QAM as its underlying modulations. The FFT size is 256 and the signal to noise ratio (SNR) ranges from 5dB - 20dB. This is shown in Figures 6 and 7 respectively. From the plot and numerical data, we observe that for both modulation schemes, SER of the legitimate receiver decreases very quickly as SNR increases. SER reaches to 0 at 14dB for QPSK modulated OFDM symbols and less than 10^{-5} at 20dB for 16-QAM modulated OFDM symbols. On the other hand, the decoding SER for the adversary stays approximately at 75% and 93.5% for QPSK and 16-QAM modulated OFDM symbols respectively throughout all SNR values. This implies the adversary's decoding successful rate is equivalent to random guessing over all QPSK and 16-QAM symbols. This shows *OFDM Enc* has achieved optimal SER for the adversary, where optimal is viewed as the adversary can do no better than random guessing.

B. Simulation 2: Performance Evaluations under Compromised Key Streams Settings

The second simulation we conducted was to compare SER of the conventional encryption scheme with *OFDM Enc* under the assumption that a portion of key streams is compromised. We have simulated three modulation schemes: QPSK, 16-QAM and 64-QAM. The FFT size is still kept at 256 and SNR level is 30dB. For QPSK modulated symbols, the required key streams between the conventional scheme and *OFDM Enc* are the same at 512 bits. In 16-QAM and 64-QAM modulated OFDM symbols, the required key stream length for the conventional scheme is 4 bits and 6 bits per subcarrier respectively. These require two times and three times of key streams of *OFDM Enc* at 1024 bits and 1536 bits respectively. As a result, we performed two simulations on the conventional encryption with 16-QAM and 64-QAM modulated OFDM symbols. First, we simulate the scenario where only the first bit of in-phase and quadrature components mapped to each subcarrier is encrypted. This is to make conventional scheme utilizing the same amount of key streams as *OFDM Enc*. We call this "Conventional Encryption with Half Key Length" for 16-QAM modulation and "Conventional Encryption with One Third Key Length" for 64-QAM modulation. In these cases, the adversary would immediately recover half and two third of the information bits. This is not secure at all! Second, we simulate the case where each message bit is encrypted by a key stream bit. We call this "Conventional Encryption with Full Key Length" for both 16-QAM and 64-QAM modulations. Moreover, when we say k "Known Keys", that implies first k pairs from key streams $\mathbf{a}$ and $\mathbf{b}$ are compromised. The results for QPSK, 16-QAM and 64-QAM modulated symbols are shown in Figures 8, 9 and 10 respectively.

For QPSK modulated OFDM symbols, SER of *OFDM Enc* scheme is slightly less than the conventional scheme, which implies the performance of the conventional scheme is slightly better. SER decreases linearly with increased compromised key streams in conventional schemes with all three modulations. This is expected because a percentage of compromised key streams directly transform into recovered messages. However, this is not the case with *OFDM Enc*. In *OFDM Enc*, each compromised pair of key stream would imply only one time domain sample is correct, which contributes to a small portion of signal being correct on each frequency. However, the correct decoding of messages will rely on all time domain samples being correct. Therefore, there is no assurance on the number of recovered bits given a certain amount of key streams are being compromised. As a result, the behaviour of *OFDM Enc* generally is not linear. This is more evident in the simulations for 16-QAM and 64-QAM. For both 16-QAM and 64-QAM modulated OFDM symbols, we can easily observe that SER is almost always higher with *OFDM Enc* when key streams of

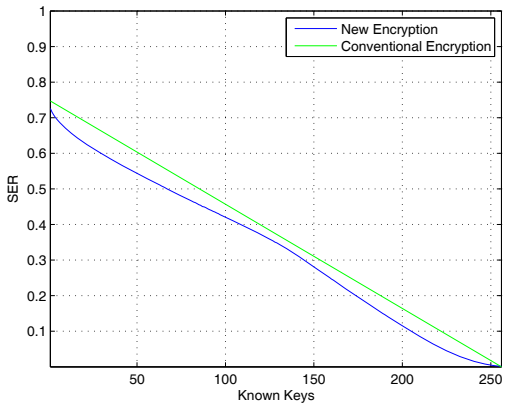

Fig. 8. Decoding SER when a Subset of Key Streams are Compromised with QPSK Modulation

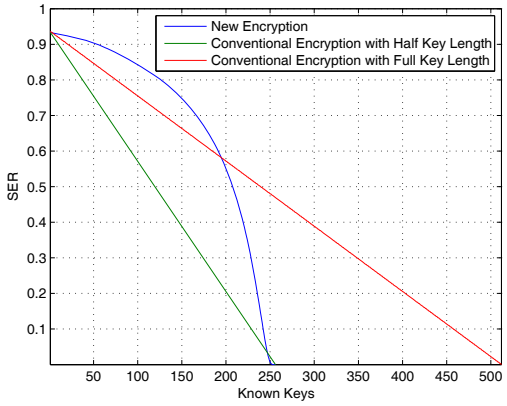

Fig. 9. Decoding SER when a Subset of Key Streams are Compromised with 16-QAM Modulation

the same length are used. SER drops very slowly initially. In some scenarios, *OFDM Enc* has better performance than the conventional scheme with full key stream length. This occurs when the blue line is above the red line in Figures 9 and 10.

For *OFDM Enc* scheme, one important note we want to point out is that in 64-QAM modulated OFDM symbols, SER is kept around 85% even though approximately 80% of key streams are compromised. We think this is a quite remarkable result. This implies that *OFDM Enc* is highly resistant to key stream compromises when higher modulation schemes are used.

From these simulations, we can conclude that performance of *OFDM Enc* is comparable to the conventional scheme at lower rate (QPSK) modulation schemes. However, it has much better performance at higher rate (16-QAM and 64-QAM) modulation schemes when the same amount of key streams is used. Moreover, the performance of *OFDM Enc* is at least comparable with the conventional scheme at full key stream length encryption until almost most key streams are compromised.

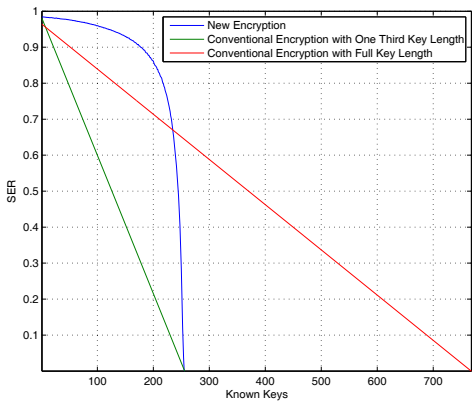

Fig. 10. Decoding SER when a Subset of Key Streams are Compromised with 64-QAM Modulation

C. Simulation 3: Performance Evaluations under Different FFT Sizes

The last simulation we performed was to see if OFDM is block size dependent, which means we want to test if using *OFDM Enc*, we get a different SER when a percentage of key streams are compromised for different FFT size N. Here, FFT sizes are chosen to be 128, 256, 512, 1024 and 2048, which corresponds to different FFT size specified in LTE [2]. The SNR level remains at 30dB. We further assume 25% of key streams are compromised with *OFDM Enc* scheme. This implies only 12.5% of key streams are compromised with full conventional encryption in 16-QAM modulated OFDM symbols. The results are plotted in Figure 11 for QPSK and Figure 12 for 16-QAM. We can see clearly that in both schemes, performance of *OFDM Enc* are not affected by the FFT size. This implies *OFDM Enc* will have the same performance when different bandwidths are assigned. Other percentage of compromised key streams were also tested to confirm this result. Note again in this particular example, as shown in Figure 12, SER of *OFDM Enc* is almost 20% higher than the conventional encryption with the same key streams and approximately 7% higher than conventional encryption with less key streams. This implies our scheme has a greater impact on the adversary in terms of the decoding SER.

VI. Conclusions and Future Work

In this paper, we have introduced a new physical layer OFDM encryption scheme which we called *OFDM Enc*. This scheme is computationally secure against the adversaries. This scheme encrypts the message by term-wise multiplication of each of the in-phase and quadrature components of time domain OFDM symbols with key streams $\mathbf{a}$ and $\mathbf{b}$, where $\mathbf{a}$ and $\mathbf{b}$ are $\{-1, 1\}$ valued binary sequences. This is equivalent to non-linear masking in the frequency domain. Furthermore, this scheme will not alter the PMEPR values of the transmitted OFDM symbols.

There are two distinct differences between the conventional encryption and *OFDM Enc*. 1) In the conventional encryption,

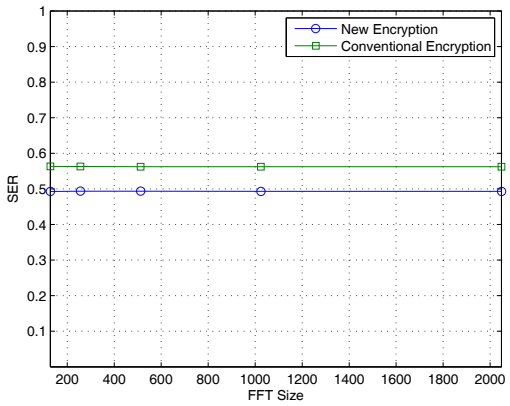

Fig. 11. Performance of QPSK Encryption with Different FFT Sizes when a Certain Percentage of Key Streams are Compromised

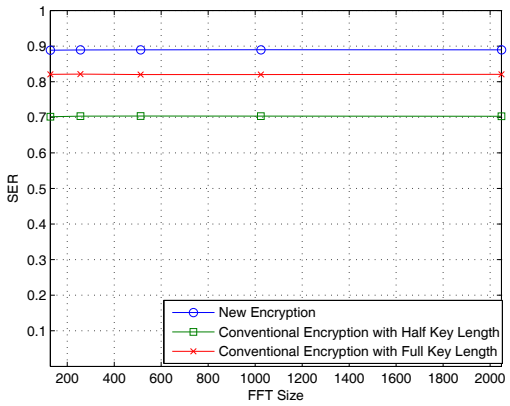

Fig. 12. Performance of 16-QAM Encryption with Different FFT Sizes when a Certain Percentage of Key Streams are Compromised

knowing one bit of keystream will guarantee the recovery of one bit message. However, for *OFDM Enc*, knowing one bit of key stream will only allow one to recover the correct sample for that time instance. Correct decoding of any message symbol relies on all time domain samples to be correct. Thus, there is no assurance on the number of recovered bits. 2) It requires less key streams compared to conventional cipher encryption. This is because in the conventional encryption, there is a one to one correspondence between the information bit and the key stream bit, any reduced key size would directly result in exposed information bits. In *OFDM Enc*, each symbol containing multiple bits are encrypted using two bits. Furthermore, the added hardware complexity is minimal. The amplitude of the sample either remain unchanged or the sign is flipped. Therefore, the proposed scheme may prove to be very useful for high speed applications in the constrained devices.

In terms of decoding SER for the adversary, simulations have shown that *OFDM Enc* would perform almost as well as conventional schemes with QPSK subcarrier modulations. It performs far superior with higher modulation schemes when using the same key stream length. Moreover, *OFDM Enc* is highly resistant to key stream compromises. Finally, *OFDM Enc* performance is not FFT size dependent.

The open questions are: (i) How to theoretically show the impact of the non-linear masking? Or equivalently, how do $\mathbf{X}'$ and $\mathbf{Y}'$ in (19) and (20) behave in the presence of key streams $\mathbf{a}$ and $\mathbf{b}$. (ii) How to theoretically show the impact of the system performance under different subcarrier modulations? (iii) Conduct a further information theoretical analysis to further validate *OFDM Enc*.

REFERENCES

[1] 3GPP TS 33.401 v11.0.1. 3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects. 3GPP System Architecture Evolution (SAE): Security Architecture. Release June 11, 2011.

[2] 3rd Generation Partnership Project (3GPP), Technical Specification Group Radio Access Network; Physical layer aspects for evolved Universal Terrestrial Radio Access (UTRA).

[3] 3GPP TR 25.913 V7.3.0 (2006-03), Requirements for EUTRA and EUTRAN.

[4] R.W Chang. Synthesis of band-limited orthogonal signals for multichannel data transmission. In *Bell System Technical Journal*, vol. 45, pp. 1775–1796, 1966.

[5] L. Chen and G. Gong. *Communication system security*, Boca Raton, USA: CRC Press, 2012.

[6] A. Chorti and I. Kanaras, Masked M-QAM OFDM: A simple approach for enhancing the security of OFDM sysmtes, In *IEEE international symposium on personal, indoor and mobile radio communications*, PIRMC '09, pp. 1682-1686, September, 2009

[7] European Telecommunnication Standard, Radio broadcasting system: digital audio broadcasting to mobile, portable, and fixed receivers, ETS 300 401, 1996.

[8] European Telecommunnication Standard, Radio broadcasting system: Digital broadcasting system television, sound, and data services Framing structure, channel coding, and modulation digital terrestrial television, ETS 300 744. 1996.

[9] B. Javidi. Noise performance of double-phase encryption compared to XOR encryption *Opt. Eng.*, vol. 38, no. 1, pp. 9–19, Janurary 1999

[10] IEEE Standard 802.16, Part 16: Air Interface for Fixed Broadband Wireless Access Systems. 2004.

[11] M. Khan, M. Asim, V. Jeoti, and R. Manzoor On secure OFDM system: Chaos based constellation scrambling In *International Conference on Intelligent and Advanced Systems*, ICIAS '07, pp. 484–488, November 2007.

[12] S. Litsyn. In *Peak power control in multicarrier communications*, Cambridge, UK: Cambridge University Press, 2007.

[13] A. Moradi, A. Poschmann, S. Ling, C. Paar and H. Wang. Pushing the limits: a very compact and a threshold implementation of AES. In *Paterson, K. (ed.)*, EUROCRYPT '11. LNCS, vol. 6632, pp. 69–88. Springer, Heidelberg (2011).

[14] N. Morelli, C.C. Kuo and M.O. Pun. Synchronization techniques for orthogonal frequency division multiple access (OFDMA): a tutorial review. In *Proceeding of the IEEE*, vol. 96, no. 7, pp. 1394–1426, July 2007.

[15] NIST, Advanced Encryption Standard (AES) FIPS Publication. 197, November 2001.

[16] R. Prasad *OFDM for wireless communication systems*, USA: Artech House Inc, 2004

[17] M.B. Pursley. In *Introduction to digital communications*, Upper Saddle River, USA: Prentice-Hall, 2005.

[18] D. Reilly and G. Kanter, Noise-enhanced encryption for physical layer security in an OFDM radio, In *IEEE radio and wireless symposisum*, RWS '09, pp. 344-347, Janurary, 2009

[19] A. Satoh, T. Sugawara and T. Aoki. High-performance hardware architecure for Galoise counter mode. In *IEEE Transactions on Computer*, vol. 58, no. 7, pp. 917–923, July 2009.