A New Efficient Physical Layer OFDM Encryption Scheme

Fei Huo
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Email. fhuo@uwaterloo.ca
Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Email. ggong@uwaterloo.ca

Abstract

Orthogonal frequency-division multiplexing (OFDM) is a multiplexing method in which data are transmitted over the equally spaced, overlapped carrier frequencies. The advantages of OFDM include: It can achieve high data rate with great bandwidth efficiency and flexible underlying modulations. It can easily eliminates intersymbol interference (ISI) with the help of cyclic prefix (CP). Channel equalization becomes much simpler compared to single carrier (SC) systems. As a result, many standards have incorporated OFDM. Moreover, in a wireless communication setting, stream cipher encryptions are usually performed by independently encrypting a message bit with a key stream bit through exclusive OR (XOR) operations. This is a generic method and can be applied to any communication systems. The required key stream length is the same as the message length. This might be problematic in a high speed data transmission application with constrained devices. The rate of generation of key streams might not keep up with the transmission rate.

In this paper, we propose a new encryption scheme specifically for OFDM systems. It requires less key streams compared with other approaches. The idea comes from the importance of orthogonality in OFDM symbols. Destroying the orthogonality will create inter-carrier interferences (ICI). ICI will affect symbols on all subcarriers. This will in turn cause higher symbol error rate (SER) and higher bit error rate (BER) for the adversary. The encryption is performed on the time domain OFDM symbols, which is equivalent to performing a nonlinear masking in the frequency domain. Various attacks will be explored in this paper. These include known plaintext and ciphertext attack, frequency domain attack, time domain attack and random guessing attack. The mutual information between plaintext and encrypted ciphertext will also be derived. Finally, simulations are conducted to compare the new scheme with the conventional approach.

Index Terms. Wireless communication, OFDM, Security, Stream cipher encryption, Tradeoffs.

1 Introduction

OFDM was first proposed by Chang [9]. It is a multiplexing method in which data are transmitted over the equally spaced, overlapped carrier frequencies. Advantages of OFDM compared to conventional SC systems 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 [6], digital audio broadcasting (DAB) [4] and digital video broadcasting (DVB) [5] just to name a few.

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 [10], 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 a wireless communication setting, stream ciphers are usually chosen for the purpose of encryption. This is primarily because data transmission over wireless channels are error prone compared to wired transmissions. In stream cipher encryptions, 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. There will not be any error propagation in the decoding process. This differs from block cipher encryption. In block cipher encryptions, one bit error in the ciphertext will cause the entire block of messages to be incorrectly decoded. Therefore, one can either choose to use a stream cipher to encrypt directly or convert a block cipher into stream cipher through counter (CTR) mode or cipher feedback (CFB) mode then perform the encryption [10].

We refer to this approach as the conventional encryption scheme in this paper. This scheme can achieve the secrecy. However, to produce one bit of ciphertext would require one bit of key stream. This could potentially create problems in a high speed data transmission application with constrained devices. For instance, in the next generation mobile 3GPP LTE standard, it has been designed to meet a downlink (DL) peak data rate of 300 Mb/s (with 4 antennas and 64-QAM modulations) [3]. As a result, the key streams generation rate has to be the same. Assuming the encryption cipher is AES [7] used in counter mode, to the best of authors' knowledge, even though the performance of AES can vary from 2.56 Gb/s to 62.6 Gb/s depending on the implementations, this would require a hardware of 34.5 Kgates and 979.3 Kgates respectively [19]. This would be 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 [15]. This is not nearly sufficient to meet the requirement set forth by LTE.

Various other encryption techniques specifically targeted for OFDM have been proposed, such as chaos based constellation scrambling [13], noise enhance approach [18] and masked approach [11]. However, none of these techniques would solve the problem described above. In the case of [18], 8 bits per subcarrier are required for the encryption, which generally requires more key streams than standard stream cipher encryption. Therefore, it is of the great interest to find a method to encrypt information with less key streams and also achieve good security levels.

In this paper, we investigate how we could more efficiently encrypt the data without compromising the security. Our contributions are summarized below:

- We propose a new physical layer encryption scheme specifically targeted for OFDM which we called *OFDM Enc*. The encryption performed on the time domain OFDM symbols. This is equivalent to performing a nonlinear masking on the frequency domain signals. The key streams required for encryption are reduced.

- An initial investigation on the security of this new scheme is conducted. Various attacks were explored. These include known plaintext and ciphertext attack, frequency domain attack, time domain attack and random guessing attack. Theoretical result on the mutual information between plaintext and ciphertext is also derived.

- Simulations were performed to compare the performance in terms of SER of *OFDM Enc* with the conventional stream cipher approach.

The encryption is performed by varying the signs of each of in-phase and quadrature component of time domain OFDM symbols according to two key streams. This will destroy the orthogonality of OFDM symbols and create ICI [16]. Without the knowledge of these signs, the adversary will have a high error probability when he tries to decode.

The rest of this paper is organized as follows. In Section 2, we will introduce the notations used throughout the paper. In Section 3, we will give some background information on OFDM systems, conventional stream cipher encryptions and decryptions. The system assumption and adversary model will also be described in this section. In Section 4, we will present detailed description on *OFDM Enc* scheme as well as the corresponding decryption scheme. In Section 5, we will perform a thorough security analysis on our newly proposed scheme. In Section 6, we will present simulation results on our scheme. Moreover, we will compare our scheme with the conventional encryption scheme in terms of SER. Finally, in the last section, we will give some concluding remarks and some future work directions.

2 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.
- 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 denote $H(X)$ to be the entropy of random variable X, and $I(X;Y)$ to be the mutual information between random variables X and Y.
- 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 through various algorithms.

3 Background

3.1 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 $\mathbf{M} = (M_0, M_1, \cdots, M_{N-1}) \in$

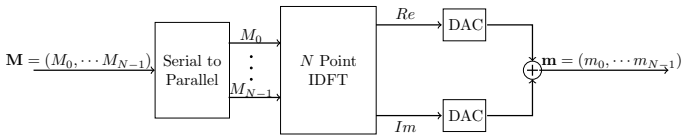


Figure 1: Baseband OFDM transmitter

$\mathbb{C}^N$ are modulated symbols to be transmitted. We assume each modulated symbol M_k is independent, identically and uniformly distributed. 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:

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

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:

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

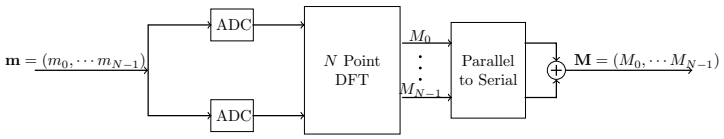


Figure 2: Baseband OFDM Receiver

3.2 Stream Cipher Encryption

When the stream cipher encryption algorithm is applied, the baseband OFDM transmitter is shown in Figure 3. Key streams **K** are first bitwise OXRed with messages **S** to produce ciphertext **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.

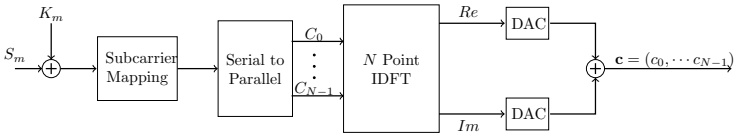


Figure 3: Conventional Stream Cipher Encryption

3.3 System Assumption

We assume two pseudorandom sequence generators (PRSG) are available to produce two key streams **a** and **b** where a_i and $b_i \in \{-1, 1\}$. This is shown in Figure 4. Each bit a_i and b_i is assumed to be independent, identically and uniformly distributed. Alternatively, one can also use one PRSG and divide into two key streams.

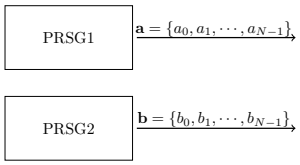


Figure 4: Pseudorandom Sequence Generators

3.4 Adversarial Model

We assume adversaries have complete knowledge of the channel. He can intercept all messages exchanged between the transmitter and the legitimate receiver. From this, he can use various techniques to try to recover keys, key streams and/or messages. We do not consider the scenario where the adversary tries to jam the communication channel. Moreover, we do not consider the scenario where the adversary can exploit the weaknesses in the stream cipher to recover keys and/or key streams, this is out of the scope of this work. We assume the stream cipher is perfectly secure.

4 OFDM Enc Scheme

4.1 Encryption and Decryption of OFDM Enc

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

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

where $i, k = 0, 1, \cdots, N-1$. This is shown in Figure 5.

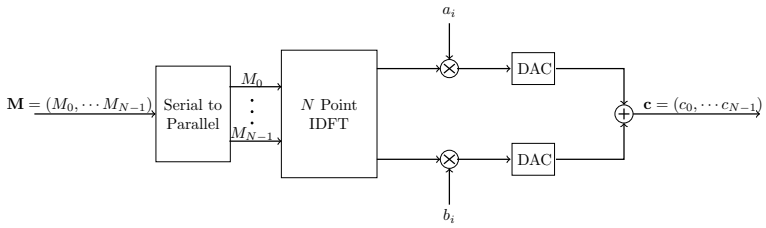


Figure 5: *OFDM Enc* Encryption

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):

$$c_i = Re\{m_i\} \times a_i + jIm\{m_i\} \times b_i. \tag{4}$$

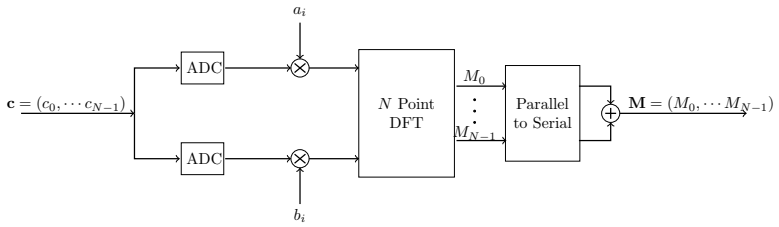


Figure 6: *OFDM Enc* Decryption

In this scheme, by potentially changing the signs of real and imaginary time domain signals, we are effectively destroying the orthogonality of OFDM symbols and thus introducing artificial ICI. Without the knowledge of these two key streams, the adversary would not be able to reverse the process to remove the interference. ICI will cause the adversary to have a high SER and BER.

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 by (4). The receiver locally generates two pseudorandom sequences $\mathbf{a} = (a_0, \cdots, a_{N-1})$ and $\mathbf{b} = (b_0, \cdots, b_{N-1})$ and computes

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

This is shown in Figure 6. After recovering $\mathbf{m}$, it follows the standard OFDM receiver structure, then 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 $\mathbf{a}$ and $\mathbf{b}$. Consequently, the adversary cannot perform the operations in (5). We will use the following example to illustrate this.

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

Encryption: We know

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

After computing 16-point FFT, we have $\mathbf{m}$ and $\mathbf{c}$ respectively in Table 1.

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 $\mathbf{M}$ and $\mathbf{S}$ to be the demodulated and decoded symbol obtained by the legitimate receiver, $\mathbf{M}'$ and $\mathbf{S}'$ to be the demodulated and decoded

Table 1: 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	$-0.346+0.048j$	$0.346-0.048j$

symbol obtained by the adversary respectively. The result is shown in Table 2. We observe in this particular example, the adversary's decoding SER is $\frac{13}{16}$ or 81.25%.

4.2 OFDM Enc and PMEPR

One major drawback of OFDM is the peak-to-mean envelope power ratio (PMEPR). This is a measurement of peak signal power to the average power. In the case where N sinusoidal signals from all subcarriers add up constructively, PMEPR could be as high as N [14]. This could be problematic to power constrained devices and power amplifier design. It is noteworthy to mention that in this scheme, by only changing the signs of time domain signals, PMEPR of OFDM symbols is guaranteed to remain unaffected. If the OFDM symbols are coded such that PMEPR property is ensured, then PMEPR of encrypted OFDM symbols is maintained. Note that all aforementioned schemes [13, 18, 11] would not guarantee this property. PMEPR of encrypted OFDM symbols will inevitably be different from un-encrypted OFDM symbols if these schemes are used.

Table 2: Decoded Messages between the Legitimate Receiver and the Adversary

$\mathbf{M}$	$\mathbf{S}$	$\mathbf{M}'$	$\mathbf{S}'$
$1-j$	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

5 Security Analysis

Conventionally, for a well designed cipher where no better than exhaustive search attack can be found, the security level would be the length of keys which generates the key streams. For this, the security level of *OFDM Enc* scheme is exactly the same as the conventional one, which would have a security level equal to the key length which generates the key stream.

5.1 Known Plaintext and Ciphertext Attacks

If the adversary knows modulated symbols $\mathbf{M}$, then he can compute the OFDM symbol $\mathbf{m}$. From (5), both a_i and b_i can be recovered. Therefore, he can recover the key streams $\mathbf{a}$ and $\mathbf{b}$. This is the same attack as the conventional stream 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 the correct time domain symbols. As a result, he can statistically estimate $\mathbf{a}$ and $\mathbf{b}$, but he is not guaranteed to recover any key streams with 100% certainty. In this case, *OFDM Enc* is likely to be more resistant against known plaintext and ciphertext attack.

5.2 Frequency Domain Attack

In this subsection, we explore the possibility of launching attacks in the frequency domain. Let F and F^{-1} be the DFT and IDFT matrix respectively shown as follows:

$$F = \frac{1}{\sqrt{N}} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & e^{\theta_N} & \cdots & e^{(N-1)\theta_N} \\ 0 & e^{2\theta_N} & \cdots & e^{2(N-1)\theta_N} \\ \vdots & \vdots & & \vdots \\ 0 & e^{i\theta_N} & \cdots & e^{(N-1)i\theta_N} \\ \vdots & \vdots & & \vdots \\ 0 & e^{(N-1)\theta_N)} & \cdots & e^{(N-1)^2\theta_N} \end{pmatrix}$$

and

$$F^{-1} = \frac{1}{\sqrt{N}} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & e^{-\theta_N} & \cdots & e^{-(N-1)\theta_N} \\ 0 & e^{-2\theta_N} & \cdots & e^{-2(N-1)\theta_N} \\ \vdots & \vdots & & \vdots \\ 0 & e^{-i\theta_N} & \cdots & e^{-(N-1)i\theta_N} \\ \vdots & \vdots & & \vdots \\ 0 & e^{-(N-1)\theta_N)} & \cdots & e^{-(N-1)^2\theta_N} \end{pmatrix}$$

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

The adversary may attempt to directly apply the DFT F on $\mathbf{c}$ as follows and then perform the decoding:

$$F\mathbf{c}^T \quad = \quad F\{(\mathbf{a} \cdot Re(\mathbf{m}))^T + j(\mathbf{b} \cdot Im(\mathbf{m}))^T\}. \tag{6}$$

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 (6). 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

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

This gives

$$Re(m_i) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (X_k \cos(\theta_N ik) - Y_k \sin(\theta_N ik)), \tag{7}$$

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

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

$$\mathbf{m}^T = F^{-1}\mathbf{M}^T \tag{9}$$

where$f_{ik} = e^{jik\theta_N}, 0 \leq i, k < N$. Writing $\mathbf{m}$ in terms of real part and imaginary part of $\mathbf{M}$, (9) becomes

$$\begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ \vdots \\ m_{N-1} \end{pmatrix} = F_{\cos}^{-1} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{pmatrix} - F_{\sin}^{-1} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_{N-1} \end{pmatrix} + jF_{\sin}^{-1} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{pmatrix} + jF_{\cos}^{-1} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_{N-1} \end{pmatrix} \tag{10}$$

where

$$F_{\cos}^{-1} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \cos(\theta_N) & \cdots & \cos((N-1)\theta_N) \\ 1 & \cos(2\theta_N) & \cdots & \cos(2(N-1)\theta_N) \\ \vdots & \vdots & & \vdots \\ 1 & \cos(i\theta_N) & \cdots & \cos((N-1)i\theta_N) \\ \vdots & \vdots & & \vdots \\ 1 & \cos((N-1)\theta_N) & \cdots & \cos((N-1)^2\theta_N) \end{pmatrix} \tag{11}$$

and

$$F_{\sin}^{-1} = \frac{1}{\sqrt{N}} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & \sin(\theta_N) & \cdots & \sin((N-1)\theta_N) \\ 0 & \sin(2\theta_N) & \cdots & \sin(2(N-1)\theta_N) \\ \vdots & \vdots & & \vdots \\ 0 & \sin(i\theta_N) & \cdots & \sin((N-1)i\theta_N) \\ \vdots & \vdots & & \vdots \\ 0 & \sin((N-1)\theta_N)) & \cdots & \sin((N-1)^2\theta_N) \end{pmatrix} \tag{12}$$

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

$$\mathbf{m}^T = (F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) + j(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T). \tag{13}$$

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

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

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:

$$\begin{aligned} \mathbf{M}^T &= (F_{\cos}^2\mathbf{X}^T + F_{\cos}F_{\sin}\mathbf{Y}^T + F_{\sin}^2\mathbf{X}^T - F_{\sin}F_{\cos}\mathbf{Y}^T) + \\ &\quad j(F_{\sin}F_{\cos}\mathbf{X}^T + F_{\sin}^2\mathbf{Y}^T - F_{\cos}F_{\sin}\mathbf{X}^T + F_{\cos}^2\mathbf{Y}^T) \\ &= (F_{\cos}^2 + F_{\sin}^2)\mathbf{X}^T + j(F_{\sin}^2 + F_{\cos}^2)\mathbf{Y}^T \\ &= \mathbf{X}^T + j\mathbf{Y}^T. \end{aligned} \tag{14}$$

The multiplication between matrices $F_{\cos}F_{\sin} = 0_{N\times N}$, where $0_{N\times N}$ is a $N \times N$ 0 matrix. This is described in the following proposition.

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., $F_{\cos}F_{\sin} = 0_{N\times N}$.*

Proof: Let $F_{\cos}F_{\sin} = M'_{N\times N}$, for $i,j \in \{1,2,\cdots,N\}$, sine $\sin(-ik\theta_N) = -\sin(ik\theta_N)$, we have:

$$\begin{aligned} M'_{ij} &= -\sum_{k=0}^{N-1} \cos(k(i-1)\theta_N)\sin(k(j-1)\theta_N) \\ &= -\sum_{k=1}^{N-1} \cos(k(i-1)\theta_N)\sin(k(j-1)\theta_N). \end{aligned}$$

Case 1. N is odd,

$$\begin{aligned} M'_{ij} = \sum_{l=1}^{(N-1)/2} & [\cos(l(i-1)\theta_N)\sin(l(j-1)\theta_N) + \\ & \cos((N-l)(i-1)\theta_N)\sin((N-l)(j-1)\theta_N)]. \end{aligned}$$

Since

$$l(i-1)\theta_N + (N-l)(i-1)\theta_N = N\theta_N = 2\pi$$

and

$$l(j-1)\theta_N + (N-l)(j-1)\theta_N = N\theta_N = 2\pi,$$

we have

$$\begin{aligned} \cos(l(i-1)\theta_N) &= \cos((N-l)(i-1)\theta_N) \\ \sin(l(j-1)\theta_N) &= -\sin((N-l)(j-1)\theta_N) \end{aligned}$$

which implies that

$$\begin{aligned} & \cos(l(i-1)\theta_N)\sin(l(j-1)\theta_N) + \cos((N-l)(i-1)\theta_N)\sin((N-l)(j-1)\theta_N) \\ = \ & \cos(l(i-1)\theta_N)[\sin(l(j-1)\theta_N) + \sin((N-l)(j-1)\theta_N)] \\ = \ & 0. \end{aligned}$$

Then we obtain $M'_{ij} = 0$ for all $0 \le i,j < N$ when N is odd.

Case2. N is even,

$$\begin{aligned} M'_{ij} = \sum_{l=1}^{(N/2)-1} & [\cos(l(i-1)\theta_N)\sin(l(j-1)\theta_N) \\ & + \cos((N-l)(i-1)\theta_N)\sin((N-l)(j-1)\theta_N)] \\ & + \cos((N/2)(i-1)\theta_N)\sin((N/2)(j-1)\theta_N). \end{aligned}$$

Terms in the summation is equal to 0 as proved in the odd case. The only difference is the extra term

$$\cos((N/2)(i-1)\theta_N)\sin((N/2)(j-1)\theta_N).$$

However,

$$(N/2)(j-1)\theta_N = (j-1)\pi$$

and

$$\sin((j-1)\pi) = 0,$$

which implies that

$$\cos((N/2)(i-1)\theta_N)\sin((N/2)(j-1)\theta_N) = 0.$$

Then we obtain $M'_{ij} = 0$ for all $0 \leq i, j < N$ when N is even.
From the discussion above, we have proved that $M'_{ij} = 0_{N\times N}$. □

Since $F_{\cos}F_{\sin} = 0_{N\times N}$. We call $F_{\cos}$ is 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

$$\mathbf{c}^T = D_{\mathbf{a}}(F_{\cos}^{-1}\mathbf{X}^T - F_{\sin}^{-1}\mathbf{Y}^T) + jD_{\mathbf{b}}(F_{\sin}^{-1}\mathbf{X}^T + F_{\cos}^{-1}\mathbf{Y}^T), \tag{15}$$

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:

$$\begin{aligned} F\mathbf{c}^T &= F_{\cos}\mathbf{c}^T + jF_{\sin}\mathbf{c}^T \\ &= (F_{\cos}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T + F_{\cos}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T + F_{\sin}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T - F_{\sin}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T) + \\ &\quad j(F_{\sin}D_{\mathbf{a}}F_{\cos}\mathbf{X}^T + F_{\sin}D_{\mathbf{a}}F_{\sin}\mathbf{Y}^T - F_{\cos}D_{\mathbf{b}}F_{\sin}\mathbf{X}^T + F_{\cos}D_{\mathbf{b}}F_{\cos}\mathbf{Y}^T), \end{aligned} \tag{16}$$

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

Here, we clearly see the differences between un-encrypted messages and encrypted messages in the view of the adversary by comparing (14) and (16). 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 (14). 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:

$$\mathbf{X}' = F_{\cos} D_{\mathbf{a}} F_{\cos} \mathbf{X}^T + F_{\sin} D_{\mathbf{b}} F_{\sin} \mathbf{X}^T + F_{\cos} D_{\mathbf{a}} F_{\sin} \mathbf{Y}^T - F_{\sin} D_{\mathbf{b}} F_{\cos} \mathbf{Y}^T \quad (17)$$

$$\mathbf{Y}' = F_{\sin} D_{\mathbf{a}} F_{\cos} \mathbf{X}^T - F_{\cos} D_{\mathbf{b}} F_{\sin} \mathbf{X}^T + F_{\sin} D_{\mathbf{a}} F_{\sin} \mathbf{Y}^T + F_{\cos} D_{\mathbf{b}} F_{\cos} \mathbf{Y}^T \quad (18)$$

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 Gaussian noise, 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 $\mathbf{a}$ and $\mathbf{b}$, 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.

5.3 Time Domain Attack

If $i = 0$, the real and imaginary portions of the OFDM symbol from (7) and (8) respectively become:

$$Re(m_0) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_k, \quad (19)$$

$$Im(m_0) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} Y_k. \quad (20)$$

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:

$$C = \binom{N}{m} \times \binom{N}{n}, \quad (21)$$

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 $N = 128$, it can be quickly calculated 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 (19) and (20).

5.4 Random Guessing of OFDM Symbols

We assume that both 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 sense, the conventional scheme is more resistant to random guessing for $r > 2$. However, for $N > 64$,

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

The smallest FFT size in LTE is $N = 128$ [3]. Thus, this attack of directly random guessing of the key stream bits is not a threat to those real systems in the standard.

5.5 Compressed Key Stream Length

If M_k is a 2^r-ary modulated symbol, in the conventional stream cipher encryption, this would require r bit key streams to 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 encryption scheme and *OFDM Enc*:

$$\epsilon = \frac{r}{2} \tag{22}$$

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.

5.6 Mutual Information between Plaintext and Ciphertext

In this subsection, we will examine the asymptotic behaviour of mutual information between time domain plaintext $\mathbf{m}$ and ciphertext $\mathbf{c}$ through theorem 1. Before we introduce theorem 1, we first prove the following lemma.

Lemma 1 *Let* $\mathbf{m}$ *and* $\mathbf{c}$ *be two vectors of length* N *whose elements* m_i *and* c_i *are defined by (1) and (4) respectively, and* $i = 0, 1, \cdots, N-1$. *Then*

$$\lim_{N\to\infty} \frac{1}{N} H(\mathbf{m}) = \lim_{N\to\infty} \frac{1}{N} H(\mathbf{c}) \tag{23}$$

Proof:

It is shown in [21] that time domain complex OFDM symbols $\mathbf{m}$ converge to a complex Gaussian random process in distribution as the number of subcarriers N becomes large. At any time instant, m_i converges to a complex Gaussian random variable with mean 0 and variance σ_S^2. The encrypted OFDM signals c_i also converge to the same complex Gaussian distribution. This is trivial so we omit the proof here. The idea of proof is that the probability distribution function (PDF) of Gaussian distributions are symmetrical along y-axis so it is only a function of the magnitude. Therefore, the same PDF is obtained even though signs might have been changed.

Moreover, from [8], it is shown for N greater than some number n_0, then convergence in distribution implies convergence of entropy. As a result, both $H(m_i)$ and $H(c_i)$ converge to $H(Z)$, where $Z \sim N(0, \sigma_S^2)$. Therefore,

$$\lim_{N\to\infty} H(c_i) = \lim_{N\to\infty} H(m_i), \tag{24}$$

Since we know

$$\frac{1}{N} H(\mathbf{c}) \geq \frac{1}{N} H(\mathbf{m}),$$

because $\mathbf{c}$ is a function of $\mathbf{m}$. On the other hand,

$$H(\mathbf{c}) \quad \leq \quad \sum_{i=0}^{N-1} H(c_i).$$

From (24), we can obtain

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} H(c_i) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} H(m_i).$$

Moreover, entropy of OFDM symbols $\mathbf{m}$ converges to sum of entropy of each individual component as N tends to infinity, then we have

$$\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}H(m_i)=\lim_{N\to\infty}\frac{1}{N}H(\mathbf{m}).$$

Consequently,

$$\lim_{N\to\infty}\frac{1}{N}H(\mathbf{c})\leq\lim_{N\to\infty}\frac{1}{N}H(\mathbf{m}).$$

Therefore, we obtain

$$\lim_{N\to\infty}\frac{1}{N}H(\mathbf{c})=\lim_{N\to\infty}\frac{1}{N}H(\mathbf{m}).$$

This completes the proof. □

Theorem 1 *The normalized mutual information between plaintext* $\mathbf{m}$ *and ciphertext* $\mathbf{c}$ *of length* N *as* N *tends to infinity is given by the following equation:*

$$\lim_{N\to\infty}\frac{1}{N}I(\mathbf{m};\mathbf{c})=r-2. \tag{25}$$

where r *represents number of bits per symbol.*

Proof: Note that entropy of time domain symbols and frequency domain symbols are identical.

$$\begin{aligned}
\lim_{N\to\infty}\frac{1}{N}I(\mathbf{m};\mathbf{c}) &= \lim_{N\to\infty}\frac{1}{N}(H(\mathbf{c})-H(\mathbf{c}|\mathbf{m}))\\
&= \lim_{N\to\infty}\frac{1}{N}(H(\mathbf{m})-H(\mathbf{c}|\mathbf{m}))\ \ (\textit{Lemma 1})\\
&= \lim_{N\to\infty}\frac{1}{N}(H(\mathbf{M})-H(\mathbf{a},\mathbf{b}))\\
&= \lim_{N\to\infty}\frac{1}{N}(H(\mathbf{M})-H(\mathbf{a})-H(\mathbf{b})) \qquad (26)\\
&= \lim_{N\to\infty}\frac{1}{N}(rN-2N) \qquad (27)\\
&= r-2.
\end{aligned}$$

(26) holds because $\mathbf{a}$ and $\mathbf{b}$ are independent. (27) holds because each element a_i, b_i and M_i in $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{M}$ respectively are independent, identically and uniformly distributed random variables. This completes the proof. □

This theorem implies the following. As N becomes large, when $r = 2$, the mutual information between the plaintext and ciphertext is 0. Thus, this scheme is optimal in the sense that perfect secrecy is achieved [20]. Theoretically, no information is leaked to the adversary. On the other hand, when higher rate modulation where $r > 2$ is used, some information will be revealed to the adversary, because message bits are encrypted with less key stream bits. This is a tradeoff between the secrecy and the efficiency.

6 Simulation Results

In this section, we have conducted several simulations in MATLAB to demonstrate the performance of *OFDM Enc* compared to the conventional stream cipher encryption. All simulation results were averaged over 10^4 OFDM symbols. Throughout all simulations, we assume the adversary tries to recover the message by directly applying the DFT on the encrypted OFDM symbols and then perform the decoding. Finally, we assume the channel to be additive white Gaussian noise (AWGN) channel.

6.1 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 7 and 8 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. This complies with channel capacity theory [12]. 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.

6.2 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

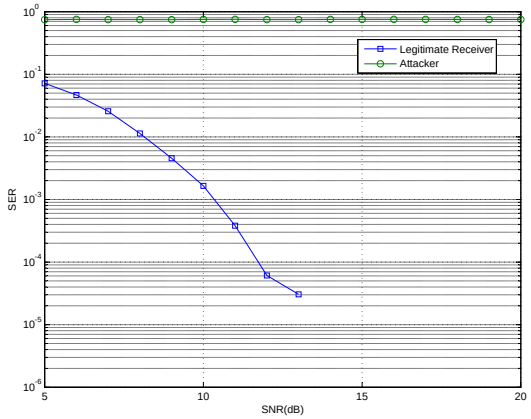


Figure 7: Performance of Legitimate Receiver and Adversary under Different Noise Level with QPSK Modulation

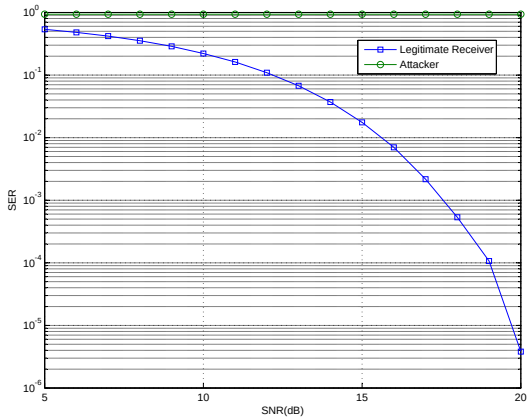


Figure 8: Performance of Legitimate Receiver and Adversary under Different Noise Level with 16-QAM Modulation

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 **a** and **b** are compromised. The results for QPSK, 16-QAM and 64-QAM modulated symbols are shown in Figures 9, 10 and 11 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. However, when we conducted simulations at lower SNRs, the offset between these two schemes become almost non-existent. SER decreases proportionally 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*. As we have discussed earlier, non-linear distortions have been introduced as a result of encryption, each compromised pair of key stream would imply only one time domain signal is correct, which contributes to a small portion of signal being correct on each frequency when DFT is performed during the demodulation. However, the correct decoding of messages will rely on all time domain signals being correct. Therefore, there will be no guarantees on the number of messages that can be recovered given a certain amount of key streams are 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 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 10 and 11.

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. This is because of the non-linear masking when ciphertext is viewed at the frequency domain.

6.3 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

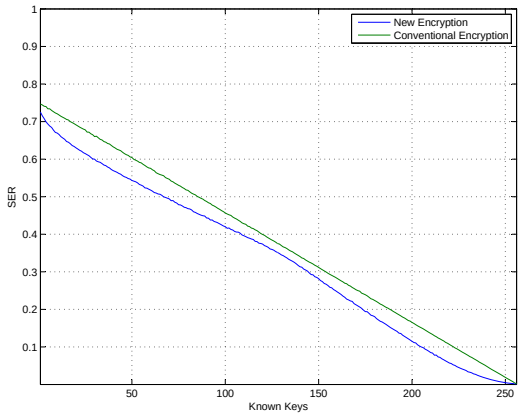
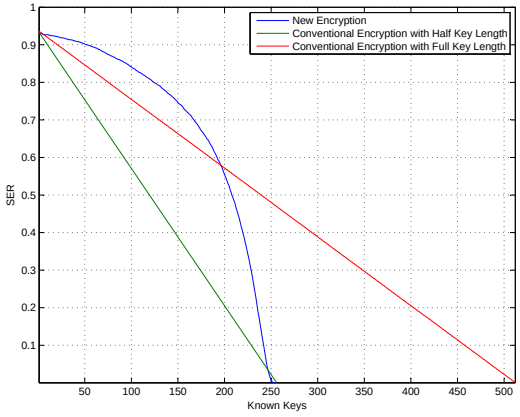


Figure 9: Performance when a Subset of Key Streams are Compromised with QPSK Modulation



h]

Figure 10: Performance when a Subset of Key Streams are Compromised with 16-QAM Modulation

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 noise level is still set to 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 12 for QPSK and Figure 13 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 13, 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 will have a greater impact on the adversary in terms of the decoding SER.

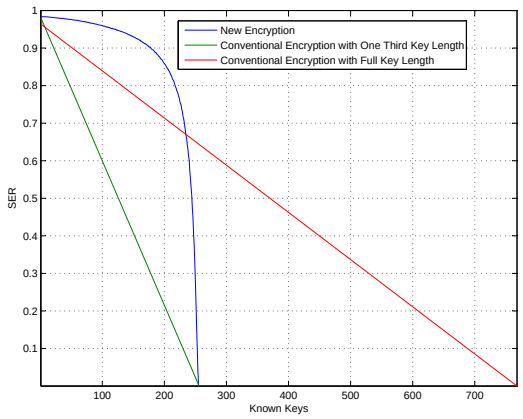


Figure 11: Performance when a Subset of Key Streams are Compromised with 64-QAM Modulation

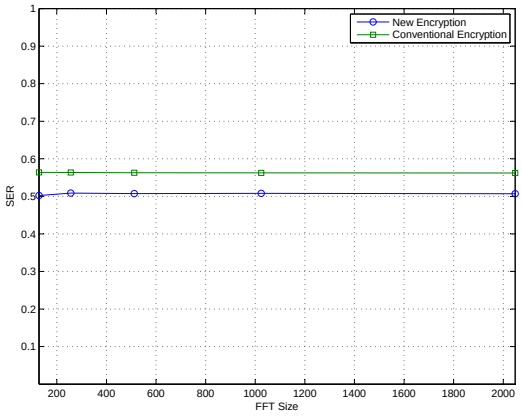


Figure 12: Performance of QPSK Encryption with Different FFT Sizes when a Certain Percentage of Key Streams are Compromised

7 Conclusions and Future Work

In this paper, we have introduced a new physical layer OFDM encryption scheme which we called *OFDM Enc*. Unlike the conventional encryption scheme where bitwise XOR are performed between messages and key streams before the subcarrier mapping and the IDFT block, *OFDM Enc* encrypts the message by term-wise multiplication of each of the in-phase and quadrature components of time domain OFDM symbols with key streams **a** and **b**, where **a** and **b** are {-1, 1} valued binary sequences. This introduces non-linear distortions for the adversary when he performs the demodulation by direct computing DFT on the received encrypted OFDM symbols without the decryption.

There are two main differences between the conventional encryption scheme and *OFDM Enc*. First, in the conventional scheme, knowing one bit of key stream will guarantee the recovery of one bit message.

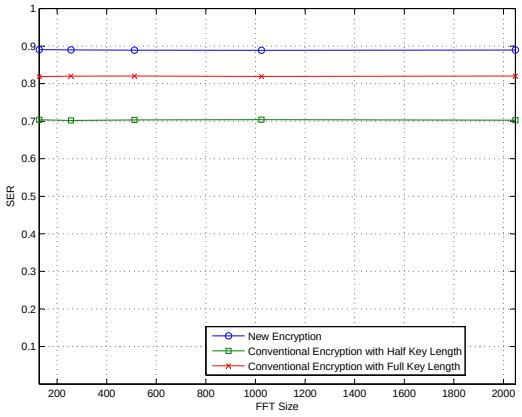


Figure 13: Performance of 16-QAM Encryption with Different FFT Sizes when a Certain Percentage of Key Streams are Compromised

However, this is not true for *OFDM Enc*. Knowing one bit of key stream will only allow one to recover the correct signal for that particular time interval. Correct decoding of any message bits relies on all time domain signals to be correct. Therefore, there will be no guarantees on how many bits can be recovered. Second, in the conventional scheme, the number of key streams required for encryption are equal to the number of message bits, which will depend on the underlying subcarrier modulation. In *OFDM Enc* scheme, the number of key streams required are 2 bits per subcarrier regardless of r. When $r > 2$, the efficiency of *OFDM Enc* is greater than one implying that less key streams are required to encrypt messages. However, it can still withstand all attacks discussed in the paper. The proposed scheme may prove to be very useful for high speed applications in the constrained devices for saving computational complexities, hardware cost and power. Furthermore, PMEPR of transmitted OFDM symbols will not be altered.

Simulations have shown that *OFDM Enc* would perform almost as well as conventional schemes with QPSK modulations. It will perform far superior with higher modulation schemes when using the same key stream length. Moreover, simulations have also shown *OFDM Enc* is highly resistant to key stream compromises. Finally, this scheme is not FFT size dependent.

In this paper, we have only presented an initial encryption framework. Much more research still need to be done. First, how do distortions affect the decision regions? Or equivalently, how do $\mathbf{X}'$ and $\mathbf{Y}'$ in (17) and (18) behave in the presence of key streams $\mathbf{a}$ and $\mathbf{b}$. Second, how will underlying modulation schemes affect the performance of *OFDM Enc*. Third, how would the performance change if the channel is not AWGN? It would be an interesting future work if these questions can be answer theoretically.

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

[5] 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.

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

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

[8] A.R Barron. Entropy and the central limit theorem. In *The Annuals of Probability*, (14)1:336–342, 1986.

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

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

[11] 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, pages 1682-1686, September, 2009

[12] T.M. Cover and J.A. Thomas. In *Elements of Information Theory*, USA: John Wiley & Sons, 1991.

[13] 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, pages 484–488, November 2007.

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

[15] 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, (6632):69–88. Springer, Heidelberg (2011).

[16] N. Morelli, C.C. Kuo and M.O. Pun. Sycnrhonization techniques for orthogonal frequency division multiple access (OFDMA): a tutorial review. In *Proceeding of the IEEE*, (96)7:1394–1426, July 2007.

[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, pages 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*, (58)7:917–923, July 2009.

[20] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, Oct. 1949.

[21] S. Wei, D.L. Goeckel and P.A. Kelly. Convergence of the complex envelope of bandlimited OFDM signals. In *IEEE Transactions on Information Theory*, (56)10:4893–4904, Octomber 2010.