IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 16, 2019, accepted December 3, 2019, date of publication December 18, 2019,
date of current version December 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960628

Analyzing Physical Layer Security of Antenna Subset Modulation as Block Encryption Ciphers

OMAR ANSARI[1], MUHAMMAD AMIN[2], AND ABRAR AHMAD[3]
[1]Electrical Engineering Department, Institute of Space Technology, Islamabad 44000, Pakistan
[2]Avionics Engineering Department, Institute of Space Technology, Islamabad 44000, Pakistan
[3]School of Engineering, Ulster University at Jordanstown, Newtownabbey BT37 0QB, U.K.

Corresponding author: Omar Ansari (omar.ansari93@yahoo.com)

ABSTRACT In this paper, a novel framework for analyzing Physical Layer Security (PLS) of Directional Modulation (DM) techniques has been introduced. The proposed framework maps the concepts of PLS techniques to cryptographic techniques, enabling the analysis of DM techniques as block encryption ciphers. The relevance of the proposed framework has been shown by applying it on Antenna Subset Modulation (ASM). After appropriate physical layer mappings, the encryption strength of ASM is analyzed using National Institute of Standards and Technology's Statistical Test Suite (NIST's STS). The performance of ASM is benchmarked against strong block encryption cipher of Advanced Encryption Standard (AES) using data types of image, text, and audio. A new metric, namely Physical Layer Randomness (PLR), has been introduced for direct comparison of encryption strength of PLS techniques to that of cryptographic techniques. The analysis shows that Optimized Antenna Subset Selection (OASS) that reduced average Side-Lobe Levels (SLLs) and improved Symbol Error Rate (SER), has rather adverse effects on encryption strength of ASM. Furthermore, it has been found that scrambling the selection of antenna subsets imparts negligible improvement in PLR.

INDEX TERMS Antenna subset modulation, directional modulation techniques, eavesdropper, intended receiver, physical layer randomness, physical layer security.

I. INTRODUCTION

Directional Modulation (DM) techniques exhibit the unique capability of wirelessly transmitting direction-dependent constellations of digital symbols which are random and encrypted along all the undesired directions, and unencrypted data is transmitted only along the desired direction. DM techniques for phased array exploit phase shifters and array weights to create desired amplitude and phase of digital modulation in the direction of Intended Receiver (IR) and random amplitude and phase in the undesired directions [1]. It is experimentally demonstrated that DM phased array generates low Symbol Error Rate (SER) along IR's direction while maintaining high SER in all the undesired directions [2], making it difficult for eavesdropper (Eve) to extract any useful information. Several other techniques have been proposed such as, Near-Field Direct Antenna Modulation (NFDAM) that creates directional information by modulating the far-field radiation pattern of antenna by changing the near-field electromagnetic boundary conditions of the antenna element (or antenna array) using high speed switches or varactors [3]. Fully-integrated transmitter for NFDAM operating at 60 GHz has been demonstrated to create directional data for secure communication [4]. Alternatively, pattern reconfigurable array based DM technique [5] requires antenna level modulation (in contrast to baseband digital modulation or phase shifters based modulation) to create desired amplitude and phase of digital modulation scheme. In [6], authors applied DM on coded signals and it is shown that higher Signal-to-Noise Ratio (SNR) is required compared to uncoded signals to extract any useful information in the undesired directions, manifesting the effectiveness of DM technique against eavesdropping on coded signals.

In Antenna Subset Modulation (ASM), introduced for secure 5G millimeter-wave wireless communication [7], directional ciphering is accomplished by randomly selecting subset of antenna array at the symbol transmission rate i.e. a new subset is selected for every symbol. However, randomly choosing subsets of antenna array has the disadvantage of high average side-lobe levels (SLLs). It is shown that

The associate editor coordinating the review of this manuscript and approving it for publication was Mohammad Tariqul Islam.

optimized selection of antenna subsets through simulated annealing [8] achieves better SER performance by reducing average SLLs along the unwanted directions. Initially, the proposed architecture of ASM was limited to phase modulation schemes only. Low-Complexity Antenna Subset Modulation (LC-ASM) [9] simplified the ASM architecture, extending its capability to accept any type of modulation scheme including Quadrature Amplitude Modulation (QAM). Iterative-FFT based ASM optimization, proposed in [10] for large-scale arrays, has been shown to not only reduce the computational complexity of optimization algorithm, but also yields higher SER (and hence assumed higher Physical Layer Security (PLS)) compared to previous optimization techniques. Multi-beams Antenna Subset Modulation (MASM) extends conventional ASM to multi-directional ASM by broadcasting beams to multiple intended receivers [11]. Interference mitigation techniques for MASM [12] focus on reducing the average SLLs in the unwanted directions by optimization of antenna subsets.

Presently in the domain of wireless communication, SER [13] and Secrecy Capacity (SC) [14] parameters are being used to measure the strength of physical layer security of DM techniques because their high values have been assumed to indicate high level of communication security and vice versa. All the optimization techniques have focused on increasing the SER and SC in the unwanted directions by reducing average SLLs [7], [10]–[18]. This paper, for the first time, shows that SLL reduction has rather adverse effect on ASM in terms of randomness and confusion.

Physical Layer Randomness probe (PLR-probe) in [19] was proposed as a new parameter for analyzing the physical layer encryption strength of DM techniques. It was shown, using the metric of PLR, that scrambling the codebook (total number of ways in which antenna subsets can be selected) after using all the possible combinations provides stronger physical layer randomness in comparison to repeated codebook. However, the analysis is limited to only one eavesdropper direction. This claim, after thorough analysis along multiple eavesdropper directions, have been investigated and found insignificant.

In this paper, an extensive investigation of ASM has been conducted by analyzing ASM as physical layer block cipher for 37 eavesdropper directions (starting from $\theta_{ED} = 0°$ to 180°, with an angle increment of $\Delta\theta_{ED} = 5°$) with highly correlated data types of image, audio and text. PLR metric has been modified to benchmark the randomness and confusion potential of ASM against modern cryptographic symmetric-key block encryption algorithm of Advanced Encryption Standard (AES).

The purpose of DM techniques is to add another security layer at the physical transmission channel, however there has not been any parameter that directly measures the encryption strength i.e. the level of randomness and confusion. PLR has been, for the first time, thoroughly analyzed in this paper to show that it is the adequate measure of randomness. Secondly, the level of randomness added by DM techniques is relative to the input data (plaintext). However as prevalent in wireless communication, randomly generated streams of data are being used as input. Since no direct measure of randomness introduced by DM techniques was being measured (instead SER and SC were being measured that supposedly showed cumulative effect of randomness of original input data and randomness introduced by DM technique), there was no way to know the effectiveness of DM technique as far as security at physical layer is concerned. In the domain of cryptography, the standard practice is to analyze the encryption strength of any encryption algorithm using highly correlated real-world data [20], contrary to randomly generated stream of data. In this work, therefore, all the analyses have been performed on highly correlated real-world data.

Following are the novel contributions of this work:

1. The framework of PLR has been modified as a benchmark metric for analysis and comparison of randomness and confusion of ASM to that of block encryption ciphers. It is shown that after appropriate physical layer mappings, the PLR of ASM can be computed and compared to encryption strength of strongest known application-layer block encryption algorithm i.e. AES. Detailed PLR analysis of ASM for different antenna subset selection techniques has been performed for all the eavesdropper directions for the first time in this work.
2. It has been shown that the conventional approach to improve PLS in ASM by reducing SLLs in unwanted directions (increasing SER and decreasing SNR) as was adopted in [7] is not correct. It has rather adverse effects on ASM in terms of randomness and confusion, as indicated by failure of multiple National Institute of Standards and Technology's Statistical Test Suite (NIST STS) randomness tests along multiple eavesdropper directions.
3. Finally it has been proven that scrambling the codebook, as was done in [19], also does not significantly enhance physical layer randomness. In some directions it does improve PLR and decreases the number of failed tests. However, it does not improve PLR to attain randomness comparable to AES in many directions.
4. Additionally, another possible selection of codebook is the combination of SLL optimized and scrambled antenna subsets, that was not investigated in [19], has also been thoroughly analyzed in this work.

The remaining paper has been organized as following: The system model for mathematically analyzing physical layer ciphering is described in Section II. PLR has been introduced in Section III. The detailed discussion on results has been reserved for Section IV. At the end of paper, conclusion and remarks are summarized in Section V.

II. SYSTEM MODEL FOR MATHEMATICALLY ANALYZING PHYSICAL LAYER CIPHERING

In this section, it is mathematically shown that Conventional Phased Array (CPA) does not provide any physical

layer security when compared with ASM that provides high level of communication security. It is followed by the concept of physical layer ciphering by DM techniques. Finally, it is mathematically shown that for Eve to extract original transmitted constellations of data in case of ASM, would require not only the relative direction of transmission but also the configuration of antenna subsets used for every symbol duration.

Suppose that Alice wants to establish point-to-point wireless communication link to Bob using a linear phased array of N isotropic antenna elements. In conventional beamforming, all the antennas of an array are ON all the time. Furthermore, it is assumed that the direction of IR i.e. Bob is known to Alice. However, Eve is situated anywhere outside the main lobe of array, as shown in Figure 1. The Array Factor in this case would be [21]:

$$AF = \sum_{m=0}^{N-1} e^{jm\psi}, \tag{1}$$

where

$$\psi = ad\cos\theta_{IR} + \beta, \tag{2}$$

and a is the wavenumber i.e.

$$a = \frac{2\pi}{\lambda}.$$

In Eq. (2), θ_{IR} is the known direction of Bob and d is the inter-element spacing taken equal to $\lambda/2$ to avoid grating lobes, β is the progressive inter-element phase difference set equal to:

$$\beta = -ad\cos\theta_{IR}, \tag{3}$$

to point the main beam in the direction of IR.

The Quadrature Phase Shift Keying (QPSK) encoded symbols are being transmitted i.e. $x = \frac{\sqrt{E_s}}{N} e^{j\phi_s(t)}$, where $\phi_s(t)$ is the phase of these symbols (i.e. *45°*, *135°*, *225°*, and *315°* degrees for *00*, *01*, *11*, *10* symbols respectively) at time t and $\sqrt{E_s}$ is the energy of each symbol which is normalized by N and given as input to each antenna element.

In antenna subset modulation, instead of using the complete array, only a subset of M ($M < N$) elements is used which is randomly chosen for every symbol transmission. The remaining $N-M$ elements remain switched OFF during that time interval. There are total possible combinations of $\frac{N!}{M!(N-M)!}$ in which the subsets of antennas could be formed. These subsets are stored in a codebook matrix (**K**) and one code vector (**k**) is used for every symbol transmission.

A. PHYSICAL LAYER CIPHERING AND CONVENTIONAL BEAMFORMING

The process of conventional beamforming has been shown in Figure 1. The main lobe is directed towards a-priori known direction of IR. The symbol X received in this direction is:

$$\begin{aligned} X &= x \times AF \\ &= \frac{\sqrt{E_s}}{N} e^{j\phi_s(t)} \times \sum_{m=0}^{N-1} e^{jm(ad\cos\theta_{IR}+\beta)}. \end{aligned} \tag{4}$$

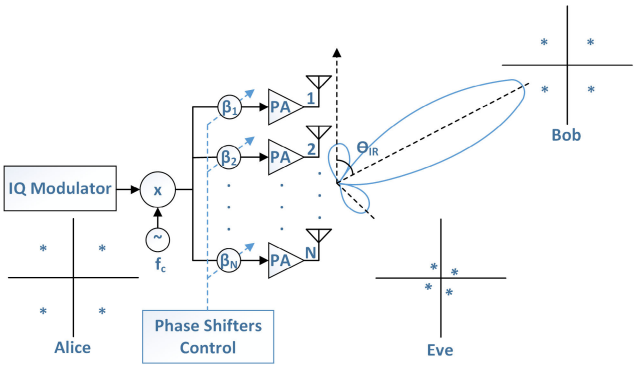

FIGURE 1. Conventional Beamforming.

Using Eq. (3), the above expression simplifies to:

$$X = \sqrt{E_s} e^{j\phi_s(t)}. \tag{5}$$

Hence Bob in the direction of θ_{IR} receives the original phase (the plaintext) of the transmitted symbol i.e. $\phi_s(t)$ with amplitude $\sqrt{E_s}$.

Now, let us consider that Eve is situated along θ_{ED}. The symbol Y received by Eve would be:

$$Y = \frac{\sqrt{E_s}}{N} e^{j\phi_s(t)} \times \sum_{m=0}^{N-1} e^{jm(ad\cos\theta_{ED}+\beta)}. \tag{6}$$

Since $\beta = -ad\cos\theta_{IR}$, we have:

$$Y = \frac{\sqrt{E_s}}{N} e^{j\phi_s(t)} \times \sum_{m=0}^{N-1} e^{jmad(\cos\theta_{ED}-\cos\theta_{IR})}. \tag{7}$$

In the above expression, since $\theta_{ED} \neq \theta_{IR}$, the phase of the original transmitted symbols is not received by Eve. Using phasor addition, Eq. (7) simplifies to:

$$\begin{aligned} Y &= \frac{\sqrt{E_s}}{N} e^{j\phi_s(t)} \times C_A e^{j\phi_{ED}} \\ &= \frac{C_A\sqrt{E_s}}{N} e^{j\phi_T(t)}, \end{aligned} \tag{8}$$

where C_A is the resultant amplitude of phasor addition of exponentials in Eq. (7) and ϕ_{ED} is the resultant phase of the array in the direction of Eve. The total phase received by Eve is $\phi_T(t) = \phi_s(t) + \phi_{ED}$, that is the summation of phase of the original symbol $\phi_s(t)$ and ϕ_{ED}. Since $C_A < N$, the amplitude of symbols received by Eve is always less than that of IR. Hence the four QPSK symbol phases received by Eve are:

$$45° + \phi_{ED},\ 135° + \phi_{ED},\ 225° + \phi_{ED},\ 315° + \phi_{ED}. \tag{9}$$

For fixed direction of Eve, the value of ϕ_{ED} remains constant. Eve can easily recover the phase of originally transmitted symbols through estimation and by using a sensitive receiver to compensate for the weak amplitude it receives. Therefore, conventional phased array does not provide any PLS.

B. PHYSICAL LAYER CIPHERING BY DIRECTIONAL MODULATION TECHNIQUES

All the DM techniques generate symbol constellations that are direction-dependent. A sharply defined constellation is transmitted only in the direction of IR. Along the rest of the directions, symbols are distorted both in amplitude and phase. The random distortion in amplitude and phase along Eve's direction is the source of physical layer ciphering in DM techniques.

In classical symmetric key cryptography, the non-encrypted message is called plaintext (P) which is acted upon by encryption (Enc) algorithm to create an encrypted message called ciphertext (C). Decryption (Dec) is performed on ciphertext using key ($\mathbf{k}$) to recover originally transmitted plaintext. In simplified form, it can be written as:

$$\begin{aligned} C &= Enc(P, \mathbf{k}) \\ P &= Dec(C, \mathbf{k}). \end{aligned} \tag{10}$$

Similarly, any DM technique can be thought of as physical layer ciphering method (just as block encryption algorithms are application layer ciphers in cryptography). DM techniques have the unique capability of transmitting encrypted message (ciphertext) along the direction of Eve and non-encrypted message (plaintext) in the known direction of IR. For instance, in ASM [7], a codebook containing the antenna subsets or keys that is changed at symbol rate is formed. Mathematically, physical layer ciphering in DM techniques can be represented as:

$$\begin{aligned} C_1 &= Enc(P_1, \mathbf{k_1}) \\ C_2 &= Enc(P_2, \mathbf{k_2}) \\ C_3 &= Enc(P_3, \mathbf{k_3}) \\ &\vdots \qquad\qquad \vdots \\ C_n &= Enc(P_n, \mathbf{k_n}), \end{aligned} \tag{11}$$

where n is the number of digital symbols of message transmitted by Alice. The above set of equations can be summarized as:

$$\mathop{\Vert}_{i=1}^{n} C_i = \mathop{\Vert}_{i=1}^{n} Enc(P_i, \mathbf{k_i}). \tag{12}$$

For Eve to extract any useful information i.e. plaintext P_i from ciphertext C_i, it would require all the keys $\mathbf{k_i}$ sequentially used by Alice for all the transmitted symbols. This process of physical layer decryption can be summarized as:

$$\mathop{\Vert}_{i=1}^{n} P_i = \mathop{\Vert}_{i=1}^{n} Dec(C_i, \mathbf{k_i}). \tag{13}$$

For ASM, it will be shown in next subsection that ciphertext C_i transmitted in the direction of Eve can be represented as:

$$\mathop{\Vert}_{i=1}^{n} C_i = e^{j\phi_s(t)} e^{j\phi_{ED}(\mathbf{k_i})} = e^{j\phi_T(t, \mathbf{k_i})}, \tag{14}$$

where $\phi_s(t)$ is the phase of transmitted symbol and $\phi_{ED}(\mathbf{k_i})$ is the randomly changing phase which requires the knowledge of keys (the antenna subsets) as well as the direction of IR, as will be shown in the next subsection.

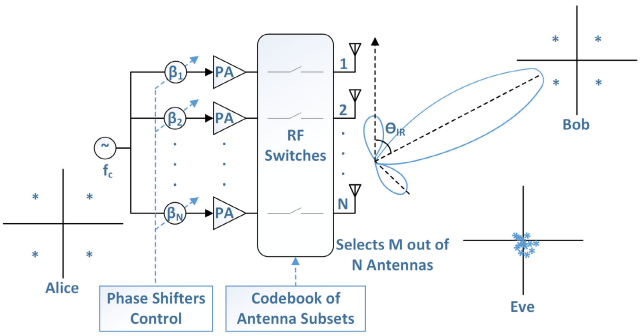

FIGURE 2. Antenna Subset Modulation - Bob receives clearly defined constellation and Eve receives symbols that are scrambled and distorted both in phase and amplitude.

C. PHYSICAL LAYER CIPHERING BY ANTENNA SUBSET MODULATION

In ASM, digital data to be transmitted is phase-modulated and fed to the phase shifters, as shown in Figure 2. The phase shifters adjust the phase of each branch and the amplified signal is fed to high-speed RF switches through power amplifiers. RF switches either turn ON or turn OFF the antennas depending on the key (antenna subset) during that symbol. Each antenna subset has the information of indices of M antennas that are to be turned ON out of N total antennas in the array. Thus the total possible combinations are $C_M^N = \frac{N!}{M!(N-M)!}$. All these combinations are stored in a codebook ($\mathbf{K}$), the dimensions of which are $C_M^N \times N$. Each element of the codebook (K_{im}) can be represented in sets notation as:

$$K_{im} = \{0, 1\}. \tag{15}$$

Every antenna subset ($\mathbf{k_i}$) can be represented as:

$$\mathbf{k_i} = [K_{i0}\ K_{i1}\ K_{i2}\ \ldots\ K_{i(N-1)}], \tag{16}$$

such that, each i^{th} row (or code $\mathbf{k_i}$) of the codebook comprises of exactly M number of 1's, that is:

$$code = \{\mathbf{k_i} | \sum_{m=0}^{N-1} K_{im} = M\}, \tag{17}$$

where i can take any values between 1 and $\frac{N!}{M!(N-M)!}$, depending upon the antenna subset selection technique.

Let's assume that Alice wants to transmit x symbol to Bob. The symbol is multiplied by array factor and the antenna subset ($\mathbf{k_i}$) for that symbol duration. The array factor in this case would be:

$$\begin{aligned} AF_k &= [e^{j0\psi}\ e^{j1\psi}\ e^{j2\psi}\ \ldots\ e^{j(N-1)\psi}]\ \times \mathbf{k_i^T} \\ &= \sum_{m=0}^{N-1} K_{im} \times e^{jm(ad\cos\theta_{IR}+\beta)}. \end{aligned} \tag{18}$$

The resulting symbol X in the direction of Bob would be:

$$X = x \times AF_k = \frac{\sqrt{E_s}}{N} e^{j\phi_s(t)} \times \sum_{m=0}^{N-1} K_{im} \times e^{jm(ad\cos\theta_{IR}+\beta)}. \quad (19)$$

In the direction of IR $\beta = -ad\cos\theta_{IR}$. Therefore, the above equation becomes:

$$X = \frac{M\sqrt{E_s}}{N} \times e^{j\phi_s(t)}. \quad (20)$$

Eq. (20) is the amplitude scaled version of Eq. (5) which shows that IR receives the original phase of symbols (plaintext) i.e. $\phi_s(t)$.

Now assume that the relative direction of Eve from the antenna array is $\phi_{ED}(\mathbf{k_i})$, where $\phi_{ED}(\mathbf{k_i})$ signifies that the relative direction of Eve with respect to antenna array varies for every symbol depending upon antenna subset $\mathbf{k_i}$. The symbol Y in this case would be:

$$Y = \frac{\sqrt{E_s}}{N} e^{j\phi_s(t)} \times \sum_{m=0}^{N-1} K_{im} \times e^{jm(ad\cos\theta_{ED}(\mathbf{k_i})+\beta)}. \quad (21)$$

Using $\beta = -ad\cos\theta_{IR}$, this expression become:

$$Y(\mathbf{k_i}) = \frac{C_A(\mathbf{k_i})\sqrt{E_s}}{N} e^{j\phi_T(t,\mathbf{k_i})}. \quad (22)$$

The phase received by Eve is $\phi_T(t, \mathbf{k_i}) = \phi_s(t) + \phi_{ED}(\mathbf{k_i})$, in which $\phi_{ED}(\mathbf{k_i})$ is the arbitrary phase that is randomly changing for every symbol duration (due to random selection of antenna subset in ASM). Eve would require not only the relative direction of IR but also the key (antenna subset) used by Alice for every symbol to extract original transmitted phase i.e. $\phi_s(t)$.

III. PHYSICAL LAYER RANDOMNESS (PLR)

In this section, physical layer randomness has been discussed as a metric for randomness of DM techniques. ASM has been analyzed using this metric and it has been found that ASM fails to ensure high degree of randomness or physical layer security. The image data and text data has PLR comparable to AES only along one direction. PLR tests fail in all the directions for audio data. Furthermore, it has been shown that SLL optimization and scrambling of codebook has adverse effects on PLR, causing significant reduction of PLR. Reconstructed images for two different Eve directions and their p-values have been included at the end of this section.

A. PHYSICAL LAYER MAPPINGS

Modern symmetric key block cipher crypto-systems e.g. advanced encryption standard consist of five main components [20]: plaintext (P), ciphertext (C), encryption algorithm (E), decryption algorithm (D), and a set of keys (**K**). These components of application layer cryptograhic systems have been mapped to physical layer security systems to define a metric of randomness/security for physical layer. The mappings are as following:

- **Mapping 1 - Plaintext Mapping:** Plaintext (P) in crypto-systems is mapped to the digital communication symbols being transmitted by a PLS system. In symmetric-key block ciphers, the bits to be transmitted are converted into blocks. Each crypto-system has specific block size e.g. *128* bits for AES. In ASM, the number of bits in each encoded symbol can be thought of as a block for that symbol duration. Therefore, block size is dependent upon modulation scheme being used e.g. for QPSK and 8-PSK block size is *2* and *3* bits respectively. In the final step of this mapping, digital symbol is assigned to each physical layer data block.
- **Mapping 2 - Ciphertext Mapping:** Ciphertext (C) in crypto-systems is equivalent to the received symbols that are randomly scrambled and distorted in phase and amplitude in the direction of eavesdropper by a PLS system.
- **Mapping 3 - Encryption Algorithm Mapping:** In this mapping, application layer encryption algorithm (E) e.g. AES [22], Data Encryption Standard (DES) [23], Rivest-Shamir-Adleman (RSA) [24] is mapped to the specific degree of randomness being exploited by a PLS system: phase shifters based directional amplitude and phase synthesis of constellations in the desired direction [6], randomly choosing M antennas out of N elements of antenna array as in ASM [7], exploitation of channel randomness for physical layer security [25], the list of pre-distributed keys to nodes for securing wireless sensor networks [26], or any degree of freedom being secretly used for providing PLS. In this paper, AES has been used as a benchmark to analyze DM technique of ASM. Following four mathematical transformations are involved in AES algorithm [27]:
  - SubBytes()
  - ShiftRows()
  - MixColumns()
  - AddRoundKey()

  There are two parts of any modern encryption algorithm; confusion and diffusion. In AES, SubBytes() opeartion introduces confusion by using Substitution-box (S-box) which is designed using highly non-linear mathematical functions. In this transformation, plaintext bytes are non-linearly substituted by ciphertext bytes using S-box. It is the only component of confusion in AES. This transformation is followed by ShiftRows(), MixColumns(), and AddRoundKey() operations. These three operations introduce diffusion by shifting block rows, by mixing columns, and by XORing the bits of data with secretly generated pre-shared keys respectively.
  Operations performed in PLS domain are mapped to equivalent transformations performed in AES to analyze ASM. The details are summarized in Table 1. AES-128, having key size of *128* bits, has been selected in this mapping. In ASM, keys are stored in the codebook. Each code/key contains the indices of antennas that are

TABLE 1. Mapping 3 - Mapping of AES encryption to equivalent PLS operations in ASM.

S. No.	AES Encryption Operation	Equivalent Physical Layer Encryption Operations in ASM
1	SubBytes()	Directional substitution of plaintext symbols into ciphertext symbols in the direction of Eve
2	ShiftRows()	Nil
3	MixColumns()	Nil
4	AddRoundKey()	Keys (antenna subsets) that are modulated at symbol rate

TABLE 2. Mapping 4 - Mapping of AES decryption to equivalent PLS operations in ASM.

S. No.	AES Decryption Operation	Equivalent Physical Layer Decryption Operations for ASM (only for Eve)
1	InvSubBytes()	Determination of direction of IR for which the original data was intended
2	InvShiftRows()	Nil
3	InvMixColumns()	Nil
4	AddRoundKey()	Exact information about the keys used by Alice for every symbol duration

switched ON during that symbol transmission. Directional substitution of plaintext symbols by ciphertext symbols in the direction of Eve in ASM is equivalent to byte substitution operation in AES. In other words, the physical layer encryption mechanism of ASM can be called Directional Substitution-box (DS-box), which is equivalent to S-box byte substitution mechanism of application layer encryption. For ShiftRows() and MixColumns(), there are no equivalent operations in ASM. Adding pre-shared unique round key after every round in AES is equivalent to changing the antenna subset after every symbol duration.

- **Mapping 4 - Decryption Algorithm Mapping:** Decryption (D) is the inverse operation of encryption. It is performed on the reception side to recover originally transmitted plaintext from encrypted data (ciphertext). AES decryption algorithm comprises of following steps:
  - InvSubBytes()
  - InvShiftRows()
  - InvMixColumns()
  - AddRoundKey()

  After reception of data blocks, the process of decryption starts. First, the bytes are inverse substituted using inverse S-box. Then the rows of block ciphertext are shifted in the reverse order by InvShiftRows() operation. Similarly, columns are shifted in the reverse order in InvMixColumns() operation and, finally, pre-shared key for that particular block is XORed in order to recover original plaintext. XOR is an involution operation (an operation that is inverse of itself, just like logical complement). Therefore, XORing the data with same bits (pre-shared key) by Bob nullifies the effect of AddRoundKey() operation which was performed during encryption.

  Equivalently, in ASM plaintext is transmitted in the direction of IR by applying compensation at the transmit side (i.e. balancing out the antenna phases of each subset by adjusting β), therefore no physical layer decryption is required along the intended direction of Bob. However, that is not the case for Eve. For Eve to decrypt the data with good fidelity, it would not only require the direction of IR but also the keys (antenna subsets) used for every symbol transmission, as summarized in Table 2.

TABLE 3. Classification of p-values into ranks and their description.

S. No.	Rank	Rank Definition	Description
1	$\zeta = 5$	$p - value \geq 0.5$	Extremely Strongly Passed
2	$\zeta = 4$	$0.4 \leq p - value < 0.5$	Strongly Passed
3	$\zeta = 3$	$0.3 \leq p - value < 0.4$	Moderately Passed
4	$\zeta = 2$	$0.2 \leq p - value < 0.3$	Satisfactorily Passed
5	$\zeta = 1$	$0.01 \leq p - value < 0.2$	Barely Passed
6	$\zeta = F$	$p - value < 0.01$	Failed

- **Mapping 5 - Key Mapping:** The set of keys (**K**), that is used in the final step of both application layer encryption and decryption (discussed in Mapping 3 and Mapping 4), is mapped to the concept of keys (antenna subsets contained in the codebook) in ASM. For AES-128 the key size is *128* bits, and for ASM key size is equal to the number of antennas N in the array. Key space of AES is 2^{128} and for ASM key space depends upon array thinning ratio. For instance, if there are $N = 30$ total antennas and out of which $M = 15$ randomly chosen antennas are ON for any symbol time, then the array thinning ratio is $M/N = 0.5$ and key space is $C_M^N = \frac{N!}{M!(N-M)!} = 1.55 \times 10^8$, which means that there are 1.55×10^8 unique possible combinations in which antenna subsets could be formed. All these combinations or antenna subsets or codes/keys are stored in the codebook (**K**).

Example: Consider an array of antennas as shown in Figure 3. The process of physical layer encryption by ASM using the above mentioned mappings will be discussed in this example. QPSK modulation is being used for transmission of digital data. Suppose that Alice wants to securely transmit a byte of value *219* to Bob situated in a known direction. Since we are using QPSK modulation scheme, the byte has to be converted into its binary value and divided into physical layer blocks of size equal to *2* bits. In this way, four blocks of binary data are formed. QPSK phases are assigned to each of the four blocks. For instance, block s_1 containing the value of *11* is assigned QPSK phase of *225°*. This completes plaintext mapping. After this, a key is selected from the codebook. The key

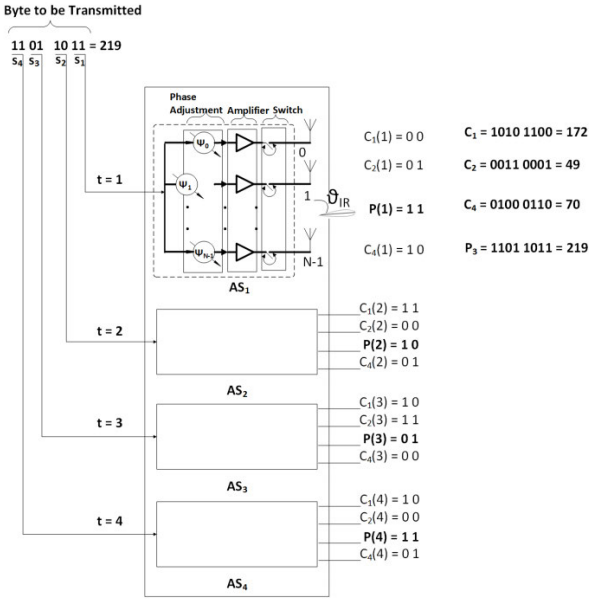

FIGURE 3. Physical Layer Encryption by ASM.

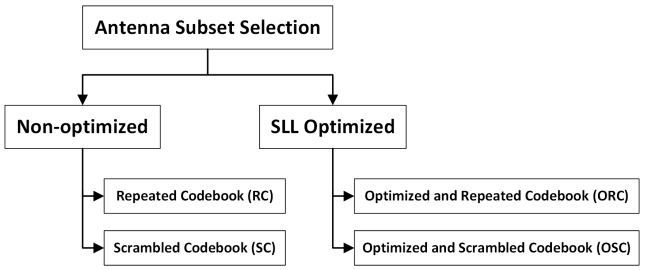

FIGURE 4. Antenna Subset Selection.

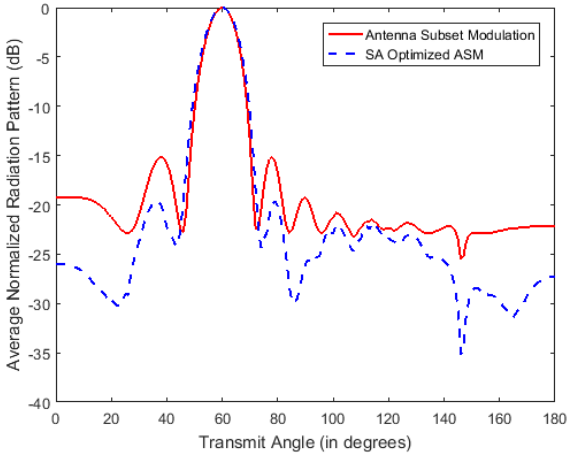

FIGURE 5. Average Normalized Radiaiton Pattern (dB) for ASM and SLL Optimized ASM using simulated annealing algorithm. The direction of IR is $\theta_{IR} = 60°$.

contains the indices of antennas that are to be switched ON during transmission of s_1 physical layer block. Each key has associated with it an array factor that introduces random phase and amplitude in the direction of Eve due to selection of random indices of antenna elements, as already described in Section II. The constellation is "substituted" (scrambled and randomized) in the direction of Eve. The same process is repeated for all the blocks in different symbol duration using different key (antenna subset). It is assumed that there are three eavesdroppers along different directions and all of them receive the ciphertext. None of them has the knowledge of keys and direction of IR in order to perform physical layer decryption. Therefore, none of them can make out the value of originally transmitted byte. The recovered ciphertext bytes by Eve are *172*, *49*, and *70*, none of which is same as plaintext byte of value *219* received by Bob. This illustrates the process of physical layer encryption in unwanted directions.

B. NIST STATISTICAL TEST SUITE

In modern cryptography, there are three commonly used randomness test suites; Dieharder battery of tests [28], TestU01 [29], and NIST STS [30]. In the development of PLR, NIST tests have been adapted owing to central importance of NIST STS as a standard for randomness analysis and benchmarking performance of AES. NIST STS is a package that analyzes randomness of binary sequences by checking the ciphertext against templates of different types of non-randomness that could exist in the binary sequences. The results of all the tests are recorded as p-values. It consists of *15* standard tests; Frequency Monobits Test (FT), Block Frequency Test (BF), Runs Test (RN), Longest Runs of Ones in a Block Test (LR), Binary Matrix Rank Test (RK), Discrete Fourier Transform Test (DT), Non Overlapping Template Matching Test (NO), Overlapping Template Matching Test (OV), Universal Statistical Test (US), Linear Complexity Test (LC), Serial Test (ST), Approximate Entropy Test (AE), Cumulative Sums Test (CS), Random Excursion Test (RE) and Random Excursion Variant Test (RV), and accordingly their p-values are denoted by; P_F, P_B, P_R, P_L, P_K, P_D, P_N, P_O, P_U, P_C, P_T, P_A, P_S, P_E and P_V. The tests which generate more than one p-values, minimum p-value is selected for simplification of analysis.

C. PHYSICAL LAYER RANDOMNESS (PLR)

The p-values of all the tests obtained by NIST STS contain vital information about randomness of ciphertext. According to statistical hypothesis testing criteria laid down by NIST, for any specific test, if $p - value < 0.01$, the null hypothesis (H_o) (i.e. the data is random) is rejected, and the alternative hypothesis (H_a) (i.e. the data is non-random) is accepted. That particular test is considered as failed and the ciphertext is declared as non-random. If $p - value \geq 0.01$, the test is considered as passed, null hypothesis (H_o) is accepted and the ciphertext is declared as random. Moreover, larger magnitude of p-value indicates the there is more randomness and confusion for the test under consideration.

In order to define PLR, ranks ζ are assigned to each p-value. If $p - value \geq 0.5$, the ciphertext is highly random

TABLE 4. Comparison of PLR of plain, AES, and ASM encrypted image along Eve direction of 35°.

Image Data	P_F	ζ	P_B	ζ	P_R	ζ	P_L	ζ	P_K	ζ	P_D	ζ	P_N	ζ	P_O	ζ	P_U	ζ	P_C	ζ	P_T	ζ	P_A	ζ	P_S	ζ	P_E	ζ	P_V	ζ	PLR
Plain	0.044	1	0.046	1	0	F	0.0003	F	0	F	0.258	2	0	F	0	F	0	F	0.406	4	0	F	0	F	1	5	0.059	1	0.441	4	18+**8F**
AES	0.426	4	0.406	4	0.253	2	0.311	3	0.03	1	0.564	5	0.41	4	0.124	1	0.316	3	0.398	3	0.079	1	0.244	2	1	5	0.361	3	0.397	3	44
ASM RC - 35^o	0.425	4	0.407	4	0.255	2	0.311	3	0.026	1	0.562	5	0.493	4	0.176	1	0.384	3	0.421	4	0.087	1	0.243	2	1	5	0.398	3	0.399	3	45
ASM SC - 35^o	0.422	4	0.403	4	0.254	2	0.312	3	0.033	1	0.560	5	0.472	4	0.185	1	0.316	3	0.436	4	0.408	4	0.079	1	1	5	0.373	3	0.397	3	47
ASM ORC - 35^o	0.421	4	0.372	3	0.253	2	0.320	3	0.023	1	0.478	4	0.136	1	0.01	1	0.047	1	0.370	3	0	F	0.248	2	1	5	0.394	3	0.403	4	37+**1F**
ASM OSC - 35^o	0.137	1	0.159	1	0.071	1	0.073	1	0.02	1	0.416	4	0	F	0	F	0	F	0.428	4	0	F	0.03	1	0.99	5	0.367	3	0.477	4	26+**4F**

TABLE 5. Comparison of PLR of plain, AES, and ASM encrypted audio along Eve direction of 45°.

Audio Data	P_F	ζ	P_B	ζ	P_R	ζ	P_L	ζ	P_K	ζ	P_D	ζ	P_N	ζ	P_O	ζ	P_U	ζ	P_C	ζ	P_T	ζ	P_A	ζ	P_S	ζ	P_E	ζ	P_V	ζ	PLR
Plain	0	F	0	F	0	F	0	F	0	F	0	F	0	F	0	F	0	F	0	F	0	F	0	F	1	5	0	F	0.605	5	10+**13F**
AES	0.427	4	0.407	4	0.25	2	0.313	3	0.024	1	0.559	5	0.399	3	0.175	1	0.372	3	0.391	3	0.055	1	0.244	2	1	5	0.369	3	0.324	3	43
ASM RC - 45^o	0.414	4	0.391	3	0.252	2	0.319	3	0.028	1	0.560	5	0.852	5	0	F	0.437	4	0.430	4	0	F	0.245	2	1	5	0.324	3	0.399	3	44+**2F**
ASM SC - 45^o	0.423	4	0.399	3	0.258	2	0.314	3	0.029	1	0.564	5	0.419	4	0.391	3	0.424	4	0.424	4	0	F	0.243	2	1	5	0.382	3	0.411	4	47+**1F**
ASM ORC - 45^o	0	F	0	F	0.024	1	0	F	0	F	0.161	1	0	F	0	F	0	F	0.406	4	0	F	0	F	1	5	0	F	0.55	5	16+**10F**
ASM OSC - 45^o	0	F	0	F	0	F	0	F	0.023	1	0.028	1	0	F	0	F	0	F	0.440	4	0	F	0	F	1	5	0	F	0.558	5	16+**10F**

TABLE 6. Comparison of PLR of plain, AES, and ASM encrypted text along Eve direction of 45°.

Text Data	P_F	ζ	P_B	ζ	P_R	ζ	P_L	ζ	P_K	ζ	P_D	ζ	P_N	ζ	P_O	ζ	P_U	ζ	P_C	ζ	P_T	ζ	P_A	ζ	P_S	ζ	P_E	ζ	P_V	ζ	PLR
Plain	0	F	0	F	0	F	0	F	0	F	0	F	0	F	0	F	0	F	0.450	4	0	F	0	F	1	5	0	F	0.667	5	14+**12F**
AES	0.428	4	0.410	4	0.253	2	0.314	3	0.025	1	0.554	5	0.389	3	0.160	1	0.408	4	0.421	4	0.09	1	0.244	2	1	5	0.391	3	0.336	3	45
ASM RC - 45^o	0.406	4	0.388	3	0.252	2	0.318	3	0.03	1	0.561	5	0.647	5	0.088	1	0.223	2	0.436	4	0.022	1	0.240	2	1	5	0.407	4	0.377	3	45
ASM SC - 45^o	0.424	4	0.403	4	0.256	2	0.311	3	0.027	1	0.561	5	0.485	4	0.379	3	0.359	3	0.379	3	0.027	1	0.244	2	1	5	0.357	3	0.355	3	46
ASM ORC - 45^o	0	F	0	F	0.094	1	0	F	0	F	0.081	1	0	F	0	F	0	F	0.377	3	0	F	0	F	1	5	0	F	0.512	5	15+**10F**
ASM OSC - 45^o	0	F	0	F	0.067	1	0.018	1	0.023	1	0	F	0	F	0	F	0	F	0.456	4	0	F	0	F	1	5	0	F	0.564	5	17+**9F**

and it is assigned a good rank of $\zeta = 5$. If $0.4 \leq p - value < 0.5$, the rank $\zeta = 4$ is assigned. The same trend is followed in assigning the ranks and *6* classes are formed as shown in Table 3. If $p - value < 0.01$, the test is considered as failed and F rank is assigned. The presence of even single F rank indicates complete failure of randomness for that PLS technique in that direction.

Definition: Physical layer randomness is defined as the cumulative sum of ranks assigned to all the NIST tests based on their p-values. Mathematically, it is expressed as:

$$PLR = \sum_{z=1}^{N_T} \zeta_z, \tag{23}$$

where N_T is equal to the total number of NIST STS tests that are performed. In our case, it is equal to *15*, since we have performed all the tests.

IV. DISCUSSION OF RESULTS

In this section, the results of PLR generated using different codebooks are presented for the case of ASM. Originally, the authors in [7] used two types of codebooks for ASM; Randomized Antenna Subset Selection (RASS) and SLL Optimized Antenna Subset Selection (OASS). Later on, the authors in [19] analyzed two more techniques of; Random and Repeated Selection (RRS), and Random and Scrambled Selection (RSS). The process of scrambling the codebook, after utilization of all the codes, effectively creates a new codebook with different sequence of codes. All these codebook types have been analyzed and benchmarked against AES using PLR metric in this section.

Antenna subset selection techniques for ASM are summarized in Figure 4. For the purpose of incorporation of two different antenna subset selection techniques from previous literature on the subject of ASM, some terminologies have been renamed for the purpose of simplification and unification of antenna subset selection techniques in this paper:

- Randomized antenna subset selection in [7] (which is same as random and repeated selection in [19]) will be referred to as Repeated Codebook (RC).
- SLL optimized antenna subset selection in [7] will be referred to as Optimized and Repeated Codebook (ORC).
- Random and scrambled selection in [19] will be referred to as Scrambled Codebook (SC).
- Moreover, another possibility of combining the two codebook selection techniques of SLL optimized antenna subsets [7] and scrambled antenna subsets [19] has also been investigated in this paper. It will be referred to as Optimized and Scrambled Codebook (OSC).

The total number of antennas are $N = 20$, out of which $M = 15$ randomly chosen antennas are ON for every symbol duration. Symbols are encoded using QPSK modulation scheme. Therefore, according to the mappings described in Section III, key size is equal to *20*, key space is $C_M^N = \frac{N!}{M!(N-M)!} = 15,504$, and block size is equal to *2* bits.

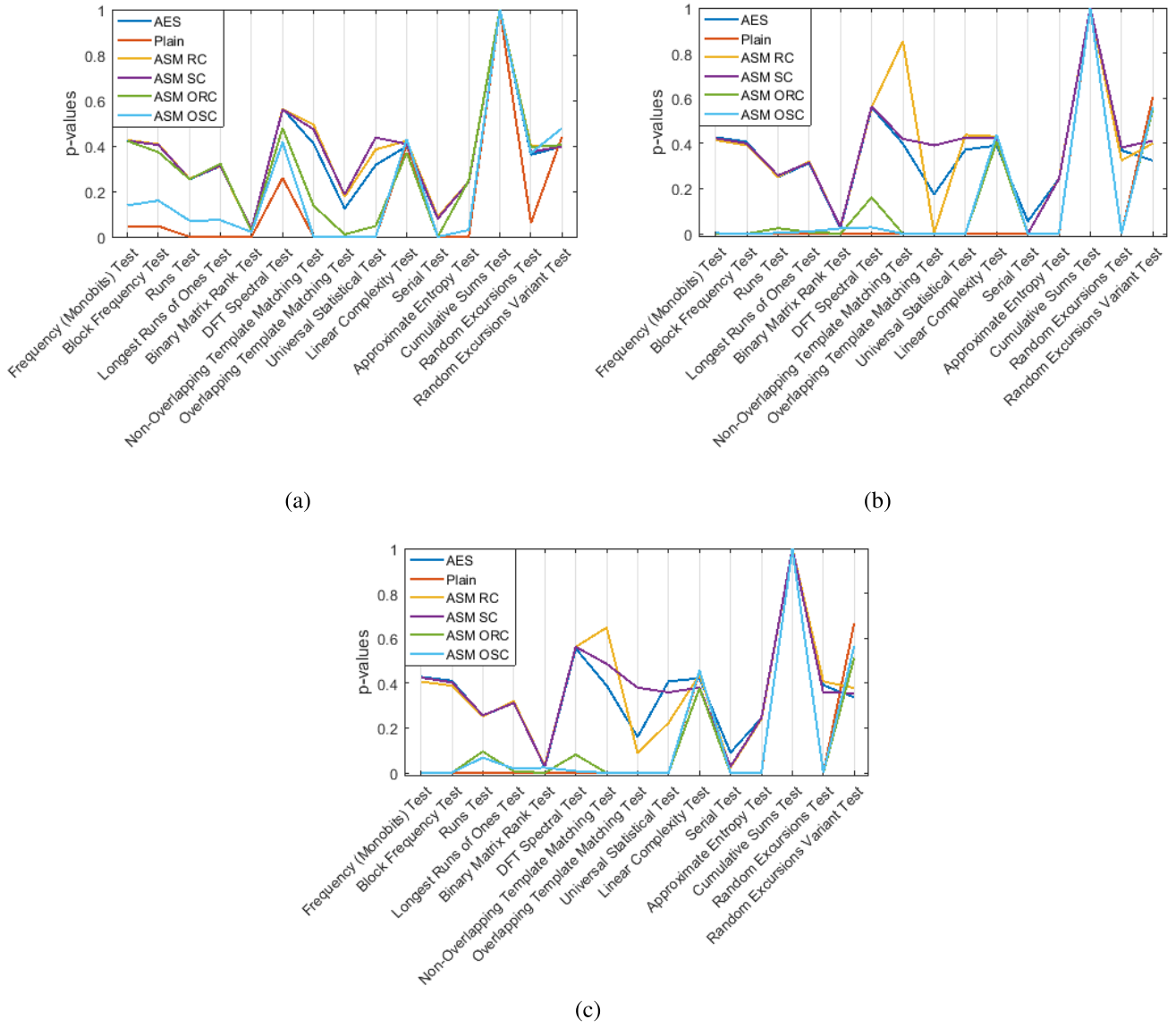

FIGURE 6. Comparison of p-values of AES with ASM for (a) Image along 35° (b) Audio along 45° (c) Text along 45°. In general, it can be observed that the magnitude of p-values tend to decrease with SLL optimization, as indicated by green and light blue solid lines in the graphs.

SLL optimization of codebook has been performed using simulated annealing algorithm, as done by authors who originally proposed OASS for ASM [7]. Simulated annealing is a heuristic optimization algorithm that seeks to find approximate global optimum in a large search space. The goal here is to synthesize the codebook containing only those antenna subsets which have low sidelobe levels in the undesired directions of eavesdropper. The cost function for optimization can be written as:

$$E = \min_{\Omega} |SLL|, \tag{24}$$

where Ω is the range of angles outside the main lobe which require minimization of radiation pattern. Exponential cooling schedule, which yields best SLL reduction for ASM [7], has been adopted in our paper. The resulting average normalized radiation pattern of ASM and SLL optimized ASM is shown in Figure 5. The process of scrambling the codebook has no effect on the average normalized radiation pattern because it only changes the sequence of keys and overall average of radiation pattern (being the sum of radiation patterns associated with all the keys) remains the same.

The transmit direction is $\theta_{IR} = 60°$. With the incremental increase of $\Delta\theta_{ED} = 5°$, Eve's position has been shifted from $\theta_{ED} = 0°$ to $\theta_{ED} = 180°$ and the data received by Eve has been analyzed using NIST STS. The evaluation of PLR from p-values by assigning appropriate ranks for image at $\theta_{ED} = 35°$, audio at $\theta_{ED} = 45°$, text data at $\theta_{ED} = 45°$ and its comparison with PLR of plaintext and AES encrypted message is shown in Table 4, 5, and 6 respectively. Plaintext image has the PLR of $18 + 8F$, indicating PLR magnitude of

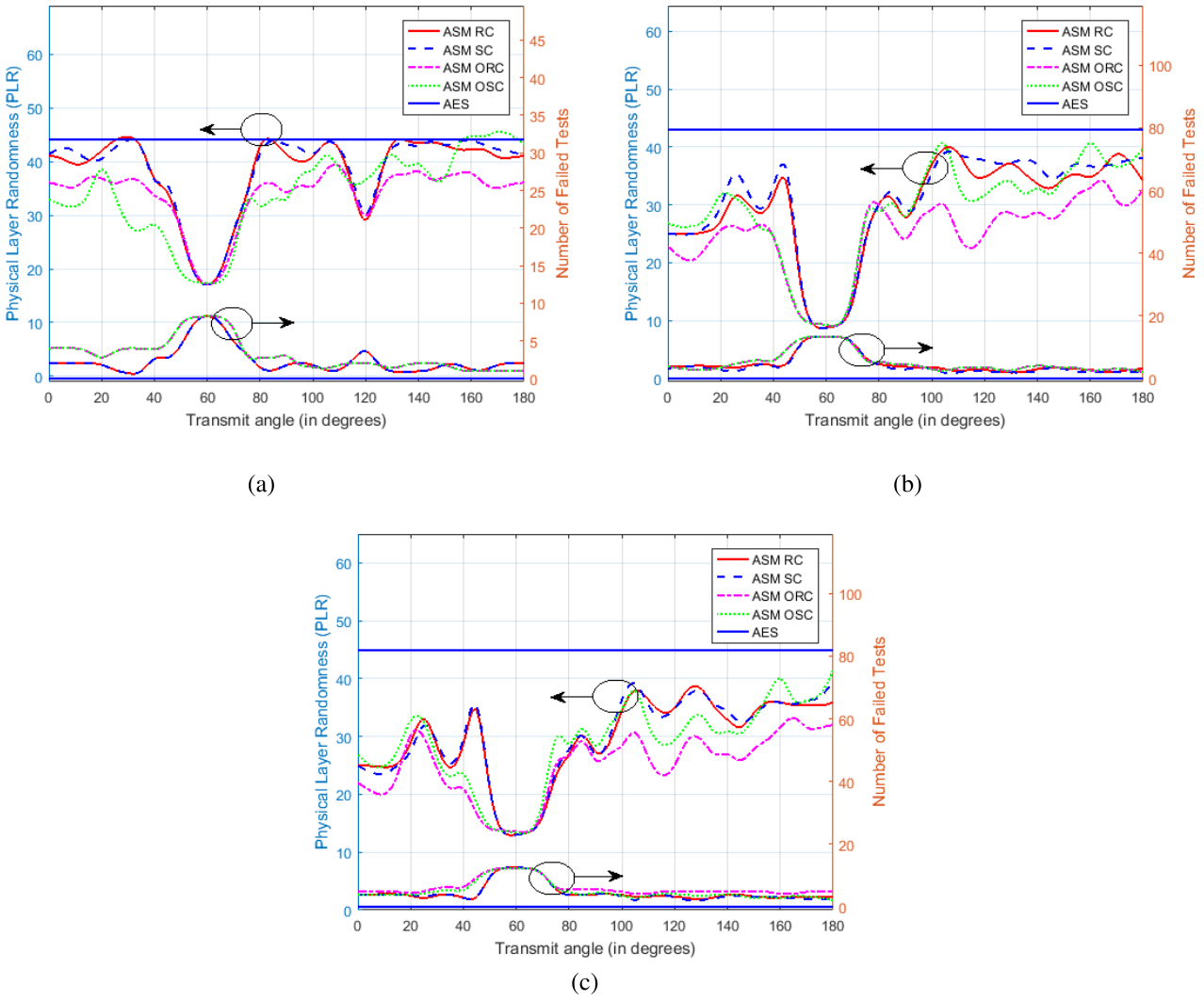

FIGURE 7. Comparison of PLR for different codebook selection of ASM with AES for (a) image (b) audio and (c) text data. In general it can be observed that randomness tends to decrease with SLL optimization as indicated by decreased PLR and increased number of failed tests for ORC and OSC.

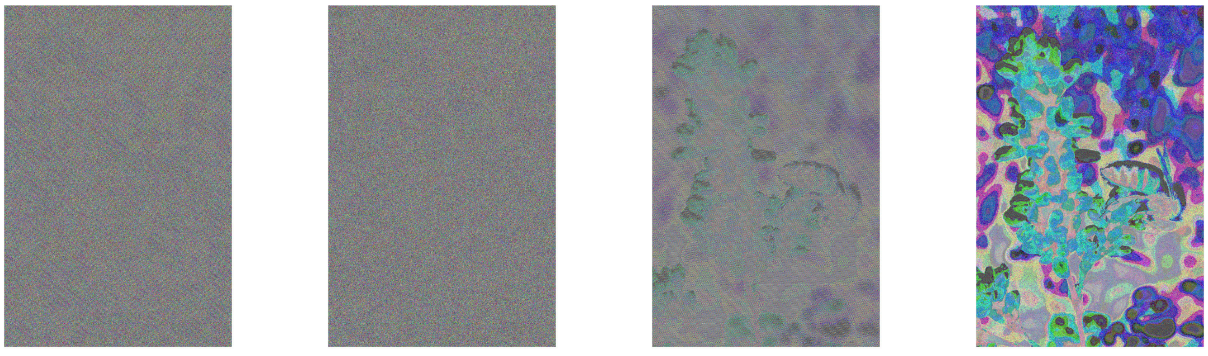

FIGURE 8. Images reconstructed by eavesdropper at angle 35° (intended direction is 60°) for (a) RC (b) SC (c) ORC (d) OSC Notice that the features of the image are most prominent (and hence least random) for OSC in (d).

18 and failure of *8* randomness tests. AES encrypted image has the PLR of *44* and zero *F* ranks. Similar calculations for audio and text data are presented in Table 5 and Table 6, respectively. A comparison of p-values of ASM encrypted message with AES for image, audio, and text data for all four codebooks is shown in Figure 6. Plaintext has the least

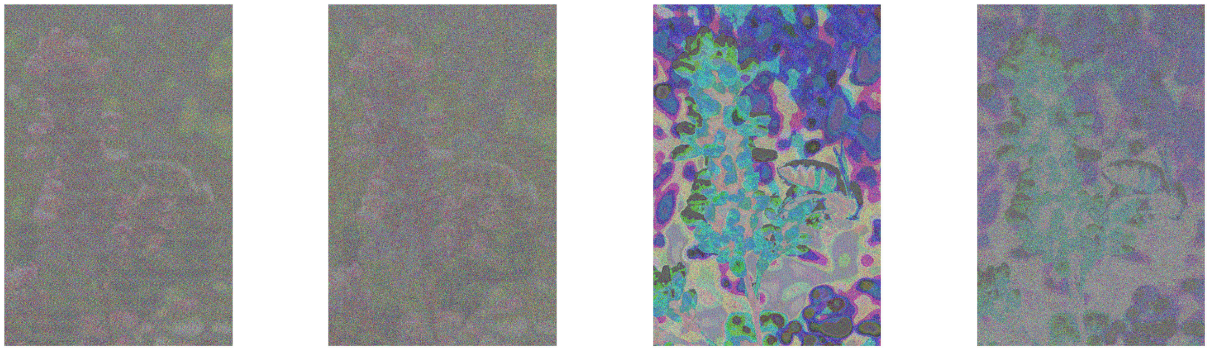

FIGURE 9. Images reconstructed by eavesdropper at angle 100° (intended direction is 60°) for (a) RC (b) SC (c) ORC (d) OSC It is noteworthy here that the image features are tangible for all the codebooks in this direction. However, the features are much more visible (and hence least random) for ORC in (c).

FIGURE 10. Reconstructed image in the direction of intended receiver along $\theta_{IR} = 60°$.

magnitude of p-values for all randomness tests. RC and SC codebooks have p-values comparable to that of AES. Furthermore, it can be observed that SLL optimized codebooks i.e. ORC and OSC have lower magnitude of p-values for all three data types compared to RC and SC.

PLR plots of image, audio and text data are shown in Figure 7. In all these graphs, the left y-axis indicates the magnitude of PLR and the number of failed tests are plotted on right y-axis. Higher value of PLR indicates higher degree of randomness and confusion. For any direction, higher the number of failed tests, lesser will be the randomness and confusion in that direction. ASM has been benchmarked against well-known application layer symmetric key block encryption cipher of AES-128 to compare its performance. Since AES is not a directional modulation technique, its PLR is same for all Eve directions. The calculations of PLR are explained in Section 3. For instance, PLR of AES encrypted image data is *44* and it does not have any failed tests in any direction, as indicated by the solid blue lines in Figure 7. Following observations can be made in Figure 7 about encryption strength of ASM:

1. PLR of repeated codebook of ASM is more or less the same as PLR of scrambled codebook and it is comparable in magnitude to PLR of AES for image data.
2. Both for ORS and OSC, PLR is lesser compared to that of RC and SC, with the exception of few directions.
3. There are no failed NIST tests only for; image data at $\theta_{ED} = 35°$, and text data at $\theta_{ED} = 45°$. Along the rest of the directions, there are one or multiple failed tests indicating the failure of physical layer security.

The images reconstructed by Eve along $\theta_{ED} = 35°$ for different types of codebook are shown in Figure 8. This is the direction for which there are no failed tests. It can clearly be seen in Figure 8 that the image is truly random (and hence secure against eavesdropping) only for RC and SC, for which the value of PLR is *45* and *47* respectively. For ORC, the image is less randomized (as also indicated by the decreased PLR of *37* and failure of serial test in Table 4). Similarly for OSC, the image features are exuberantly visible (as also indicated by decreased PLR of *26* and failure of non-overlapping template matching test, overlapping template matching test, universal statistical test, and serial test in Table 4). Along $\theta_{ED} = 100°$, the images are shown in Figure 9, in which similar observations of PLR reduction for ORC and OSC can be made. In the direction of IR along $\theta_{ED} = 60°$, the reconstructed image (plaintext) is shown in Figure 10. It has the least magnitude of PLR i.e. *18* and *F* ranks for *8* randomness tests.

Similar observations can be made about audio and text data in Table 5 and Table 6, respectively. Along $\theta_{ED} = 45°$ for audio data, PLR decreased from *47* (for SC) to *16* (for ORC and OSC) and the number of failed tests increased from *1* to *10*. Similarly, along $\theta_{ED} = 45°$ for text data, PLR decreased from *46* (for SC) to *17* (for OSC) and the number of failed tests increased from *0* to *9*. PLR plots in Figure 7 (b) for audio data and Figure 7 (c) for text data are also indicating the same. It can be observed that there is significant reduction of PLR and higher failed tests for ORC and OSC compared to RC and SC for ASM.

Clearly, performing SLL optimization (ORC and OSC) on antenna subsets in ASM has rather adverse effects on physical layer randomness for all the data types of image, audio and text, contrary to what was implicitly assumed in [7] based on the parameter of SER. The main reason for this adverse effect is that by forming the codebook containing only those antenna subsets which yield low sidelobe level properties, the key space (or size) of codebook is considerably reduced (in our case from *15*, *504* to only *272* antenna subsets). By optimizing the codebook for low SLL, all the keys (antenna subsets in case of ASM) which have large SLL properties are discarded. The codebook is limited to contain only those antenna subsets which have low SLL properties. This cause reduction of usable combinations of antenna subsets and hence the size of antenna subsets codebook. The smaller size of codebook means that there are lesser number of usable keys, the effect of which is reflected upon diminished physical layer randomness. Furthermore, the process of scrambling the codebook (i.e. SC) does not enhance the PLR notably. In some directions, it does improve the magnitude of PLR and decrease the number of failed tests. However, it does not improve the PLR enough to attain randomness comparable to AES in all the directions, as evident by the comparison of solid red line for RC and dotted blue line for SC in Figure 7. Therefore, scrambling the codebook as claimed in [19] does not actually increase the physical layer randomness.

V. CONCLUSION

The physical layer security of Antenna Subset Modulation (ASM) has been analyzed as block encryption ciphers for the first time in this paper. Analogous to the five components of symmetric-key block encryption ciphers, appropriate physical layer mappings are defined for ASM. After successful mappings, ASM is analyzed using p-values based standard randomness tests. Ranks are assigned to each p-value and the cumulative sum of ranks is introduced as a new metric, namely Physical Layer Randomness (PLR). This approach bridges the gap between conventional data encryption and modern physical layer security techniques by offering a common framework for direct comparison of randomness. It has been found that sidelobe level optimization of ASM results in reduction of encryption strength as indicated by reduced PLR. This is due to significant reduction of key space or size of codebook (possible combinations in which antenna subsets could be formed). Furthermore, it has been found that scrambling the codebook after utilization of all the keys imparts negligible improvement in PLR. The analysis, therefore, renders both sidelobe level optimization and scrambling as ineffective antenna subset selection techniques for the improvement of physical layer security of ASM, contrary to implicit assumption of physical layer security improvement based on symbol error rate characteristics in the previous literature. Clearly, some other technique for improving randomness of ASM (i.e. selection of antenna subsets) needs to be devised, for which PLR is to be used as standard parameter.

REFERENCES

[1] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.
[2] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.
[3] A. Babakhani, D. Rutledge, and A. Hajimiri, "A near-field modulation technique using antenna reflector switching," in *IEEE Int. Solid State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2008, pp. 188–605.
[4] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," IEEE J. Solid-State Circuits, vol. 43, no. 12. Singapore: Springer, Dec. 2008, pp. 2674–2692.
[5] M. P. Daly and J. T. Bernhard, "Beamsteering in pattern reconfigurable arrays using directional modulation," *IEEE Trans. Antennas Propag.*, vol. 58, no. 7, pp. 2259–2265, Jul. 2010.
[6] M. P. Daly and J. T. Bernhard, "Directional modulation and coding in arrays," in *Proc. IEEE Int. Symp. Antennas Propag. (APSURSI)*, Spokane, WA, USA, Jul. 2011, pp. 1984–1987.
[7] N. Valliappan, A. Lozano, and R. W. Heath, Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.
[8] A. T. V. Murino and C. S. Regazzoni, "Synthesis of unequally spaced arrays by simulated annealing," *IEEE Trans. Signal Process.*, vol. 44, no. 1, pp. 119–123, Jan. 1996.
[9] N. N. Alotaibi and K. A. Hamdi, "A low-complexity antenna subset modulation for secure millimeter-wave communication," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.
[10] C. Chen, Y. Dong, X. Cheng, and N. Yi, "An iterative FFT-based antenna subset modulation for secure millimeter wave communications," in *Proc. IEEE ICNC*, Silicon Valley, CA, USA, Jan. 2017, pp. 454–459.
[11] A. Akl, A. Elnakib, and S. Kishk, "Broadcasting multi-beams antenna subset modulation for secure millimeter-wave wireless communications," *Wireless Pers. Commun.*, vol. 97, pp. 3503–3517, Dec. 2017.
[12] A. Akl, A. Elnakib, and S. Kishk, "Antenna array thinning for interference mitigation in multi-directional antenna subset modulation," *Phys. Commun.*, vol. 26, pp. 31–39, Feb. 2018.
[13] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
[14] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. Singapore: Springer, 2013.
[15] L. Zhang, Y.-C. Jiao, Z.-B. Weng, and F.-S. Zhang, "Design of planar thinned arrays using a Boolean differential evolution algorithm," *IET Microw., Antennas Propag.*, vol. 4, no. 12, pp. 2172–2178, Dec. 2010.
[16] J.-F. Hopperstad and S. Holm, "Optimization of sparse arrays by an improved simulated annealing algorithm," in *Proc. Int. Workshop Sampling Theory Appl.*, 1999, pp. 91–95.
[17] R. L. Haupt, "Thinned arrays using genetic algorithms," *IEEE Trans. Antennas Propag.*, vol. 42, no. 7, pp. 993–999, Jul. 1994.
[18] M. T. Ali, R. Abdolee, and T. A. Rahman, "Decimal genetics algorithms for null steering and sidelobe cancellation in switch beam smart antenna system," *Int. J. Comput. Sci. Secur.*, vol. 1, no. 3, pp. 19–26, Oct. 2007.
[19] A. Ahmad, M. Amin, and M. Farooq, "Analyzing directional modulation techniques as block encryption ciphers for physical layer security," in *Proc. IEEE Wireless Commun. Netw. Conf.*, San Francisco, CA, USA, Mar. 2017, pp. 1–6.
[20] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 2001.
[21] C. A. Balanis, *Antenna Theory: Analysis and Design*. Hoboken, NJ, USA: Wiley, 2005.
[22] *Announcing the Advanced Encryption Standard (AES)*, Standard Publication 197, Federal Information Processing, Nov. 2001.
[23] S.-J. Han, H.-S. Oh, and J. Park, "The improved data encryption standard (DES) algorithm," in *Proc. 4th Int. Symp. Spread Spectr. Techn. Appl.*, vol. 3, Sep. 1996, pp. 1310–1314.
[24] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[25] E. Jorswieck, L. Lai, W.-K. Ma, H. V. Poor, W. Saad, and A. L. Swindlehurst, "Guest editorial: Signal processing for wireless physical layer security," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1657–1659, Aug. 2013.

[26] A. Mehmood, M. M. Umar, and H. Song, "ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks," *Ad Hoc Netw.*, vol. 55, pp. 97–106, Feb. 2016. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2016.10.007
[27] J. J. Soto, "Randomness testing of the advanced encryption standard candidate algorithms," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 6390, 1999.
[28] R. G. Brown, "Dieharder: A random number test suite, version 3.31.1," Dept. Duke Univ. Phys., Durham, NC, USA, Tech. Rep., 2004.
[29] P. Lecuyer and R. Simard, "TestU01: AC library for empirical testing of random number generators," *ACM Trans. Math. Softw.*, vol. 33, no. 4, p. 22, 2007.
[30] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, NIST Special Publication, Tech. Rep. 800-22 Rev. 1a, 2010.

OMAR ANSARI received the B.E. degree in electrical engineering from the University of Engineering and Technology, Taxila, Pakistan, in 2015, and the M.S. degree (Hons.) in electrical engineering with specialization in RF and microwave from the Institute of Space Technology, Islamabad, Pakistan, in 2019.

He is currently serving as a Graduate Research Assistant with the Institute of Space Technology, where he is involved in the design and development of millimeter-wave front end for high altitude platform (HAP). His research interests include, but are not limited to, directional modulation techniques for physical layer security, antenna design, RF circuits, and electromagnetics.

MUHAMMAD AMIN received the B.E. degree in avionics from the PAF College of Aeronautical Engineering, NED University, Karachi, Pakistan, in 1988, the master's degree in electrical engineering with specialization in high-frequency techniques from Ruhr University, Bochum, Germany, in 1998, and the Ph.D. degree from Queen's University Belfast (QUB), Belfast, U.K., in 2006.

He taught as an Assistant Professor with the College of Electrical and Mechanical Engineering, National University of Sciences and Technology, Rawalpindi, Pakistan, from 1998 to 2002. He was a consultant with TDK Electronics to develop phased array antenna for automotive collision avoidance radar. He was a Research Fellow with QUB for approximately one year and an Associate Professor with the Institute of Space Technology (IST), Islamabad, Pakistan, from October 2007 to October 2009. From October 2009 to December 2014, he was the Head of the Antenna and EMI/EMC labs, Satellite Research and Development Centre, Lahore (SRDC-L), Pakistan, where he was involved in developing monopulse tracking system for satellite and EMI/EMC space qualification tests of the satellite communications system. Since 2015, he has been a Professor with IST, the Head of the Avionics Department, and the Director of the Cyber and Information Security Lab (CISL). His research interests include the development of antennas for radar and cellular communication systems, novel techniques for modulation, and RCS reduction. His research work has resulted in over 70 publications in major journals and refereed national and international conferences. He is the inventor of a lowest profile dual polarized antenna. He is mentioned in "Marquis Who is Who in the World" 2008 edition published in USA.

ABRAR AHMAD received the B.E. degree in electronics engineering from COMSATS Abbottabad, Pakistan, in 2012, and the M.S. degree in electrical engineering from the Institute of Space Technology (IST), Islamabad, Pakistan, in 2016. He is currently pursuing the Ph.D. degree in electrical engineering with specialization in the modeling of wireless communication channel with Ulster University at Jordanstown, U.K.

In 2016, he joined the Department of Electrical Engineering, MY University, Islamabad, as a Lecturer, and in 2018, he joined IST, Islamabad, as a Lecturer.