Telecommunication Systems (2022) 79:17–32
https://doi.org/10.1007/s11235-021-00853-3

An efficient and secure cipher scheme for MIMO–OFDM systems based on physical layer security

Reem Melki[1] · **Hassan N. Noura**[2] · **Ali Chehab**[1]

Accepted: 20 October 2021 / Published online: 10 November 2021

Abstract

Multiple-input multiple-output orthogonal frequency division multiplexing (MIMO–OFDM) is, currently, the most dominant air interface for wireless communications, and the basic foundation for many network standards, due to its practicality and efficiency at high data speeds. Specifically, this system combines the MIMO and OFDM technologies, to achieve maximum capacity, reliability and throughput. On the other hand, achieving data confidentiality over wireless links in MIMO–OFDM systems, remains a pressing issue that should be tackled. In this paper, we propose an efficient and secure cipher scheme for MIMO–OFDM systems, based on the randomness and dynamicity of the physical layer. In particular, a channel-based parameter, which is extracted from the shared wireless channel, is combined with a secret key, only known to the communicating devices, to generate a dynamic key. This key is, then, used to derive two simple cipher primitives, which are a masking sequence and a permutation table. Both of these cipher primitives are updated frequently to enhance the security and robustness of transmitted data and prevent attacks. The proposed solution is considered very efficient and lightweight since it consists of simple operations, mainly, addition and permutation. Moreover, the proposed solution takes into consideration the OFDM frame symbol length, which can be fixed or varying from one antenna to another. Therefore, the proposed solution consists of two cipher variants, one secures OFDM symbols having the same length (same number of modulation symbols) and the other secures OFDM symbols that have different lengths on different antennas. Finally, several security and performance tests are conducted to prove the efficiency and robustness of the proposed solution.

Keywords MIMO–OFDM systems · Physical layer security · Security analysis · Cryptanalysis · Secure wireless communication

1 Introduction

In order to cope with the increasing demand for multi-media applications, such as high quality audio and video, specific requirements, that are related to throughput and reliability, should be met [1].

✉ Reem Melki
rmm71@aub.edu.lb

Hassan N. Noura
hassan.noura@univ-fcomte.fr

Ali Chehab
chehab@aub.edu.lb

1 Department of Electrical and Computer Engineering, American University of Beirut, Beirut, Lebanon

2 FEMTO-ST Institute, CNRS, Univ. Bourgogne Franche-Comté (UBFC), Belfort, France

Currently, OFDM is the most popular multi-carrier multiplexing method, and it is being widely-used for the transmission of wireless signals in many existing and emerging communication systems. It is also expected to maintain its dominance in future systems. Specifically, this technology transmits data over parallel narrow sub-channels, thus, converting frequency selective channels to multiple flat fading sub-channels. OFDM offers many advantages, few of which are adapting to severe channel conditions, reducing inter-symbol interference and inter-carrier interference, and achieving high spectral efficiency. However, there still exists several other network constraints that should be further addressed and enhanced, namely network capacity, coverage and channel-quality. One way to overcome these constraints, is by combining the OFDM technology with the MIMO system [2,3].

The MIMO system utilizes multiple antennas at the transmitter and the receiver to relay data, efficiently. Moreover, it operates in two modes in order to achieve either spatial multiplexing (capacity gain) or diversity gain [4]. In the former case, the same data is transmitted on multiple antennas, which enhances system reliability. Whereas in the latter case, different data are conveyed using different antennas, consequently, higher data rates are attained, without requiring additional bandwidth or increased transmit power [5]. As a result, integrating OFDM in MIMO systems results in a high performance system, that is able to achieve high reliability and increased throughput, while benefiting from the various properties of OFDM.

In order to ensure the proper functioning of MIMO–OFDM systems, robust security should be provided. Recently, physical layer security (PLS) has emerged as a promising methodology for securing wireless communication systems. Specifically, communicating users exploit the random and dynamic nature of wireless physical channels to secure transmitted data. Several PLS solutions have been presented in the literature for OFDM and MIMO systems [2,6]. In [3,7], the authors present a survey of PLS schemes that are used to detect active attacks in massive MIMO systems and how to achieve data confidentiality. The authors of [8] study the secrecy performance of two classic relaying schemes in massive MIMO systems, the amplify-and-forward, and the decode-and-forward techniques. The same approach was followed by the authors of [9–11]; they used mathematical expressions of secrecy outage probability and optimization to achieve PLS in MIMO systems. Whereas the work presented in [12–14] present a tutorial on PLS schemes for MIMO systems.

Most of the presented solutions in the literature suffer from vulnerabilities and limitations, and they are based on strict assumptions. Therefore, new security approaches should be studied and proposed.

In this paper, we propose two cipher variants for MIMO–OFDM systems that are based on PLS. The main goal is to enhance the confidentiality of data transmitted over wireless links, without introducing a large overhead. Unlike the work in the literature, we combine two concepts which are conventional cryptography and emerging PLS. This allows us to overcome the limitations of traditional, multi-round and multi-operational schemes. The first cipher variant can adopted when OFDM frame symbols have different lengths among different antennas, whereas the second variant is used when all OFDM frame symbols have a common and fixed length. Both schemes are lightweight and efficient since they are based on simple cipher primitives (permutation and masking) with simple operations. The used cipher primitives are derived from the random and dynamic properties of the physical channel (wireless), and a private key (secret). For every new frame or set of frame symbols, new cipher primitives are generated using an update process, which consists only of a permutation operation. This continuous update enhances further the security level and guards against different attacks. Finally, several security and performance evaluation tests have been presented to validate the high security level and efficiency of the proposed schemes.

The rest of the paper is organized as follows. Section 2 presents the table of notations and the MIMO–OFDM system model. Section 3 reviews the existing PLS OFDM and MIMO schemes in the literature. Section 4 describes the proposed dynamic key derivation function and the cipher primitive construction process. Section 5 proposes two novel cipher variants for MIMO–OFDM systems. Section 6 includes various security tests, which prove the security and robustness of the proposed schemes. Section 7 presents a detailed cryptanalysis discussion for the proposed schemes in the context of different confidentiality attacks. Section 8 evaluates the performance of the proposed cipher variants in terms of latency and error propagation. Finally, Sect. 9 concludes the paper.

2 Background

This section presents the table of notations and the MIMO–OFDM system model.

2.1 Notation

Table 1 represents the table of notations.

2.2 MIMO–OFDM system model

In principle, a narrow-band flat fading MIMO system is modelled as:

$$Y = H \cdot X + z, \tag{1}$$

where X and Y are the transmit and receive vectors, H is the channel matrix and z is the noise vector, respectively.

For transmitting data across a given channel, the MIMO encoder uses one of two available space time processing techniques, which are: space time coding and spatial multiplexing [15]. The first technique ensures a maximum diversity gain, where multiple copies of the same information are sent across independent fading channels to combat fading and enhance system reliability. In contrast, spatial multiplexing provides a high multiplexing gain (Degrees of Freedom (DoF)), since each spatial channel carries independent (different) information, thereby increasing the data rate [16]. The maximum spatial multiplexing order (number of independent streams) in a multiple antenna configuration is equal to [16]:

$$DoF = min(nt, nr), \tag{2}$$

Table 1 Notations

Notation	Definition
F	OFDM frame
FS	OFDM frame symbol
DK	Dynamic key
S	A masking sequence
CS	An update permutation table for S
π	Permutation table at the modulation symbol level
π_{FS}	A permutation table for π after every FS
π_F	A permutation table for π after every F
n	Number of frame symbols in one frame
l	Number of modulation symbols in one frame symbol
π^{-1}	Inverse permutation table
π_{nt}	Permutation table at the frame symbol level
π_{update}	An update permutation table for π_{nt}
nt	Number of antennas at the transmitter
nr	Number of antennas at the receiver
$(\cdot)$	Matrix multiplication
$\oplus$	Exclusive-OR (XOR)
H	Channel matrix
z	Channel noise
X	Transmit vector
Y	Receive vector
j^2	-1

where nt and nr are the number of antennas at the transmitter and receiver, respectively. Throughout the paper, we assume that $nt = nr$.

In recent years, the MIMO–OFDM system has been considered as a potential technology for enhancing the performance of different wireless transmission networks in terms of data rate and capacity, without requiring any additional bandwidth or power [15]. The main advantage of introducing the OFDM technology in MIMO systems is that it efficiently utilizes the spectrum and eliminates the effect of multipath fading. Specifically, all of the blocks of OFDM such as: FFT (Fast Fourier Transform), IFFT (Inverse Fast Fourier Transform) and CP (Cyclic Prefix) are applied to every single transmit and receive antennas as shown in Fig. 1. The output size of the IFFT/FFT blocks (size of OFDM frame symbols, which consist of a specific number of modulation symbols) can be vary between different antennas, since independent OFDM operations are carried out at each antenna. In this paper, the conventional MIMO–OFDM system is implemented using spatial multiplexing.

3 Literature review

In this section, existing PLS schemes that target MIMO and OFDM systems, are listed and discussed.

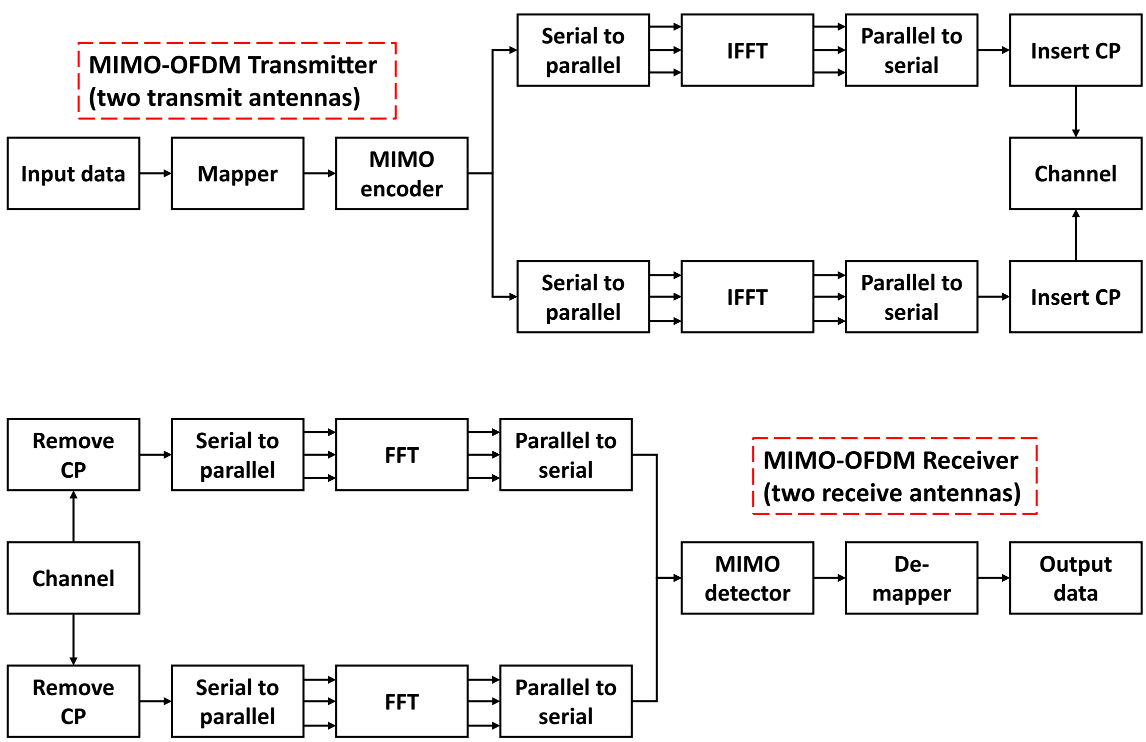


Fig. 1 A 2×2 MIMO–OFDM system

3.1 PLS schemes for OFDM systems

Several PLS schemes, that ensure data confidentiality in OFDM systems, have been presented in the literature. These schemes are split into seven groups.

3.1.1 Channel-based encryption

Most of the existing schemes in the literature exploit the randomness of wireless channels to secure the information relayed between users. In particular, communicating entities estimate and use channel state information (CSI) to encrypt/decrypt data. One approach is choosing the active subcarriers for transmitting data, based on the extracted channel parameters [17,18]. Another method is inserting dummy data within the legitimate data to baffle the adversary [19]. In contrast, the main idea behind the technique presented in [20] is to modify the traditional IFFT/FFT blocks according to the channel-related information between legitimate users.

Since wireless channels are highly random, this class of techniques can ensure high levels of security, however, on one condition, that is when channel parameters are unknown to all users except the legitimate users. In practice, channel-related information can be easily acquired when synchronizing to transmitted data and performing preamble detection.

3.1.2 Artificial noise (AN) and artificial fast fading (AFF)

These security techniques follow the same methodology of extracting and utilizing the CSI to pre-equalize transmitted messages. The added noise will be automatically eliminated when passing through the intended channel (legitimate user's channel), therefore, no additional operations are needed at the receiving end [21,22].

Similar to the first class of schemes, eavesdroppers can acquire channel-based information, which compromises the performance of these techniques.

3.1.3 Preamble modulation

In order to estimate and extract the CSI from the wireless channel between two legitimate users, the eavesdropper should detect the exchanged packet preambles, and synchronize to the communicating entities. To overcome this issue, several PLS schemes, that secure/encrypt packet preambles, have been presented in the literature [23]. A direct approach would be encrypting the packet preamble using a key only known to the transmitter and receiver. In this way, only the legitimate receiver will be able to decrypt and, thus, obtain the correct CSI. Another technique presented in this field is appending random training sequences generated by the legitimate users instead of the publicly known short and long training sequences [20].

Preamble modulation is a beneficial technique to secure CSI, however, additional security layer should be employed to protect the content of transmitted packets.

3.1.4 Encryption and PAPR reduction

The PLS scheme, presented in [24,25], jointly decreases the Peak-to-Average Power Ratio (PAPR) and enhances the security of the system, using chaotic maps. Although chaotic mapping overcomes the effect of high PAPR due to its high randomness level, it is considered computationally complex since a lot of resources are needed. A different method is the PAPR reduction scheme. Using this scheme, several pseudo-random sequences are generated and then multiplied by the transmitted symbols (post modulation symbols). Afterwards, the sequence having the lowest PAPR value is transmitted. Like the previous scheme, this method is considered inefficient since it results in a high overhead in terms of computational costs and complexity [26].

3.1.5 Permutation

Random permutation or interleaving is a conventional technique, used to achieve data confidentiality. In order to realize PLS-based permutation, a random cyclic delay or perturbation, based on the CSI between users, can be applied [27]. Differently, authors in [28] have proposed shuffling the OFDM sub-channels based on the legitimate user's channel, whereas authors in [29] have suggested permuting the complex symbols themselves.

Generally, permutation is considered as simple and efficient technique since it requires a one round and one operation to ensure security. However, static permutation tables are vulnerable to numerous types of attacks.

3.1.6 Jamming-based encryption

Authors in [30] present a novel jamming-based encryption technique, in which a legitimate receiver sends a random jamming signal, while the transmitter is transmitting information. At the receiver's side, the same random jamming signal, which was sent previously (noise), is removed/subtracted to obtain the desired data. One major drawback is that the receiver can be easily detected and jammed, thus jeopardizing the availability and confidentiality of transmitted data. Moreover, the technique presented in [30] assumes that true data can be recovered by simply removing/cancelling the jamming signal. In most cases, jammed data is corrupted and can not be recovered, hence, jamming-based schemes are not a practical approach. Also, this method is considered very complex and computationally exhaustive since it requires additional resources and overhead, which is not suitable for emerging resource-limited devices.

3.1.7 Phase encryption

The phase encryption scheme, presented in [31], is performed at the time-domain signal level. Basically, two pseudo-random sequences are generated, where one sequence is multiplied by the real part of the time domain signal, and the other is multiplied by the imaginary part. Consequently, this results in the pseudo-random phase shuffling of the in-phase and quadrature symbol components. Phase encryption is a modified version of the permutation scheme. It requires two additional operations, hence, more overhead is introduced.

3.2 PLS schemes for MIMO systems

Different PLS schemes, that target data confidentiality in MIMO systems, have been presented in the literature.

Generally, PLS schemes can be divided into six main groups which are: (1) channel-based scrambling matrices [32], (2) AN and AFF [33,34], (3) CSI [35], (4) jamming [36], (5) beamforming [37] and (6) interference based on simultaneous transmission [38]. Each of these schemes has several advantages, but suffers from multiple limitations. One main disadvantage that is common to all of the presented schemes, is the lack of secrecy in terms of using a shared secret key for encrypting the transmitted data. The shared key cannot only depend on the channel between users, since it can be known by an eavesdropper, in case of proper synchronization to transmitted data. Also, the presented schemes are case-dependent and cannot be generalized; some require perfect synchronization, others require large distances between legitimate users and eavesdroppers and many depend on the channel information, solely. Hence, we propose, next, a data confidentiality scheme that combines the notions of secrecy and dynamicity to improve the security of MIMO–OFDM systems.

4 Proposed key derivation scheme

In this section, the proposed key derivation function is described, and it is based on the work presented in [39–41].

Benefiting from the random and dynamic nature of wireless channels, end-to-end communicating devices are, now, able to secure the conveyed data between them, using PLS. Specifically, this approach has recently emerged as novel security technique that enhances the robustness of wireless communication, while maintaining low cost and overhead. Consequently, many research work has shifted towards exploring this field, and proposing novel techniques that target all security services.

In general, the security and robustness of a data confidentiality scheme is directly related to the utilized secret key (mainly referred to as encryption/decryption key). Consequently, this part of the paper presents the proposed key derivation function, which generates a set of channel-based dynamic keys, using the shared (common) physical channel and a private/secret key (known to communicating users). It should be noted that the secret key can be pre-shared between users using any traditional key distribution technique or using a Public Key Infrastructure (PKI).

First, the transmitter and receiver estimate the wireless channel between them. Then, they extract unique features and properties that are specific to their physical channel. Some of these properties include the channel state information, received signal strength and carrier frequency offset. These parameters are usually estimated by the communicating users for different communication purposes. Moreover, we make us of these parameters to generate a channel-based nonce, which will then be combined with a pre-shared secret key to generate a dynamic key. Consequently, we do not introduce any overhead for generating the channel-based nonce. The extracted parameters are pre-processed to produce a binary sequence, which is hashed. The hashing operation is crucial since any modification in any of the parameters will lead to a different nonce and consequently, to a different dynamic key. Typically, a set of common channel parameters (end-to-end) are selected according to the considered network. These parameters can be different for different networks with different characteristics. Based on these parameters, features can be extracted by applying statistical measures (such as minimum, maximum, average, and standard deviation). Afterwards, these features can be converted to a binary sequence. It should be noted that there exists several wireless channels between two MIMO users when employing spatial multiplexing. In this case, users can estimate all of the available wireless channels, extract the channel properties of multiple channels, and then combine them to enhance further the security level. From these properties, both users are able to derive the same channel-based nonce, independently. In case of channel non-reciprocity, reconciliation is applied. Any user outside the proximity of the legitimate users, is not able to derive the same channel-based nonce since the channel is viewed differently (different properties). However, this cannot be generalized. In particular, several works in the literature have proven that adversaries can derive the same channel properties as the authorized users, when having sufficient resources and power [2,39]. Thus, one should not only rely on channel information to secure a communication session.

In order to overcome this limitation, the pre-shared secret key is combined (Exclusive-OR (XOR)) with the nonce (pseudo-random and dynamic), to obtain a dynamic key. The resulting key will be used to secure the transmitted data in MIMO–OFDM systems. The SHA-512 hash algorithm is used, following the XOR operation, to make sure that the resulting key is irreversible (one-way property).

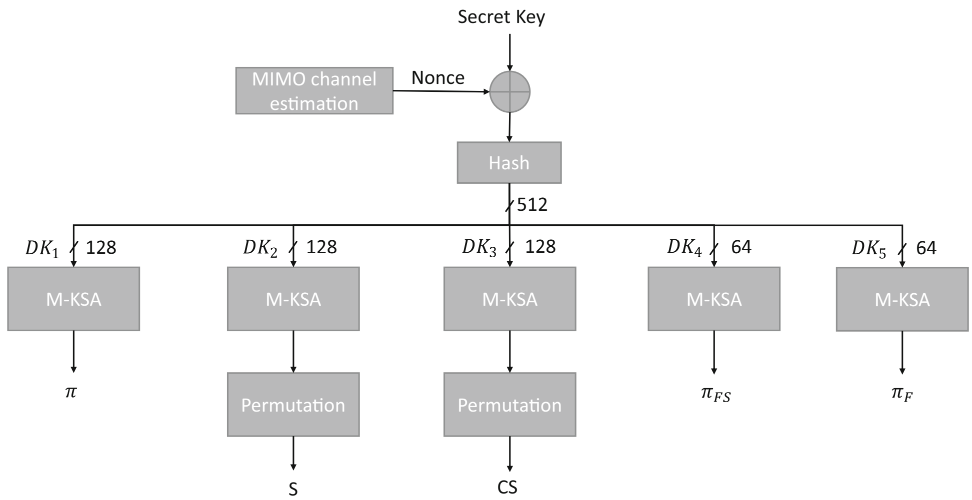


Fig. 2 The derivation procedure of the dynamic key and the construction technique of the cipher primitives for the proposed second variant (case 2)

From the 512-bit dynamic key, several sub-keys can be produced. Since the proposed solution considers two cases: (1) frame symbols having different lengths on different antennas ($l_1, l_2, l_3, \ldots, l_{nt}$) and (2) frame symbols having the same length (l), two sub-key derivation functions are proposed (cipher primitive derivation functions).

4.1 Case 1: frame symbols of different lengths

In the first case, the frame symbols on each antenna branch are assumed to have different lengths, whereas the second case assumes that all frame symbols have the same length, l. Both of these cases are real-case scenarios in existing communication systems. The first case is more challenging than the second case, hence, a simple cipher scheme with simple cipher primitives is proposed. Specifically, the 512-bit dynamic key is split into two sub-keys (256 bits each).

- The first sub-key is used to generate a permutation vector (table), π_{nt}, of length equal to $nt \times 1$ and random values between 1 and nt (number of antennas). This vector is used to permute the frame symbols on each antenna in a pseudo-random manner.
- The second sub-key is used to produce another permutation table, π_{update}. However, this table is used to permute/update the first permutation table for every new set of frame symbols (both permutation tables having the same size).

4.2 Case 2: frame symbols of the same length

As shown in Fig. 2, the obtained dynamic key in the second case is divided into five sub-keys:

- *First sub-key*: DK_1 (128 bits) is used to generate a permutation table π. It contains $nt \times l$ elements that have randomized values between 1 and $nt \times l$. This table is used to permute/shuffle the 2-D data matrices, having dimensions equal to $nt \times l$ (nt columns and l rows), at the modulation symbol level. Here, nt is the number of antennas at the transmitter's side and l is the number of modulation symbols in one OFDM frame symbol.
- *Second sub-key*: DK_2 (128 bits) is used to derive a sequence, S, having a length equal to $2 \times l$ and pseudo-random values of -1 and 1. S is used to perform masking (phase shuffling) on each frame symbol (l modulation symbols), independently. Moreover, S is divided into two vectors, S_1 and S_2, each having a length of l. The first sequence S_1 modifies the phases of the real components in complex symbols. Whereas S_2 modifies the phases of the imaginary components. In other words, the phase of the real component and the phase of the imaginary component of every modulation symbol are modified based on one element in S_1 and one element in S_2, respectively. Hence, $2 \times l$ values are needed so that each component in FS (l complex modulation symbols) is modified based on a unique value in S_1 and S_2. Note that phase modification refers to modifying the $+$ and $-$ signs of the complex symbols. If the value in S_1 or S_2 is 1, the phase of the component remains the same. In contrast, when the value is negative the phase of the corresponding component is flipped.
- *Third sub-key*: DK_3 (128 bits) is used produce a sequence CS, that includes $2l$ elements having random values between 1 and $2l$. This sequence is used to randomly shift S for every set of nt frame symbols (circular shift).
- *Forth sub-key*: DK_4 (64 bits) is used to generate a permutation table, π_{FS}, to permute π for every set of nt frame symbols.
- *Fifth sub-key*: DK_5 (64 bits) is used to generate a permutation table, π_F, to permute π for every frame.

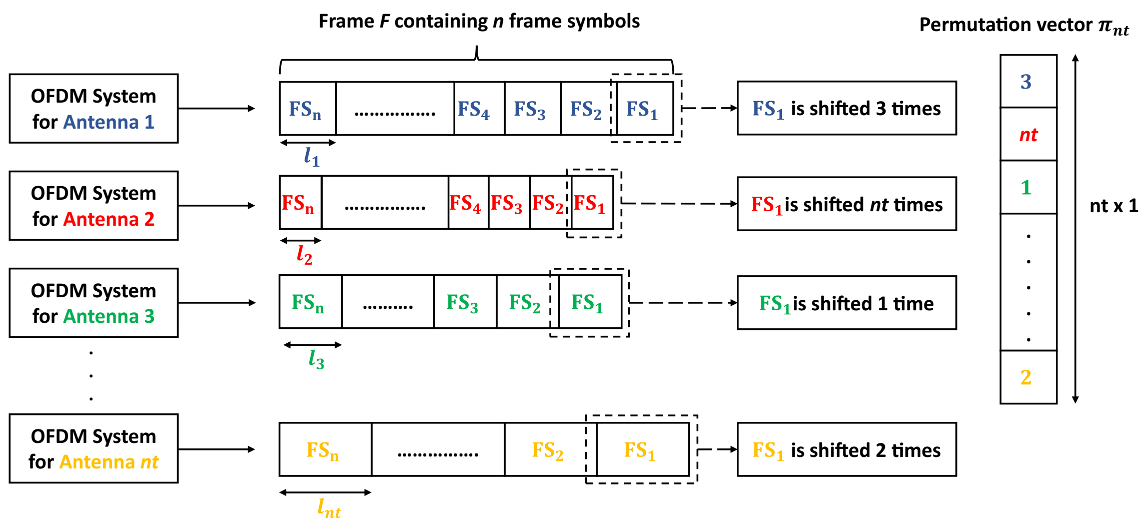


Fig. 3 Proposed data confidentiality scheme: Case 1

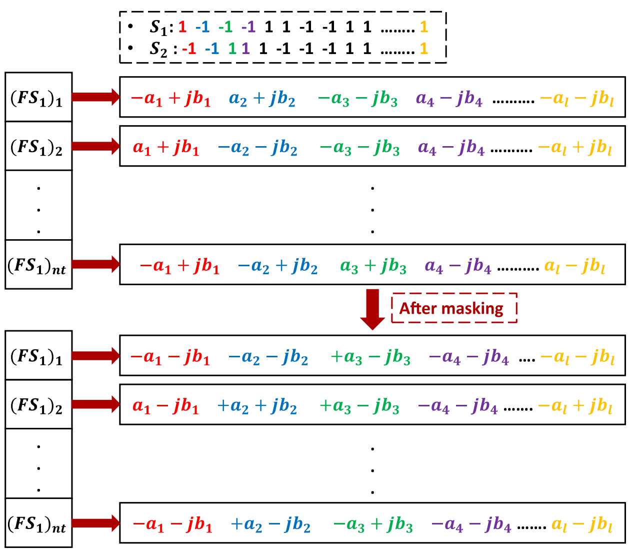


Fig. 4 Proposed masking operation

From the channel-based dynamic key, simple and lightweight cipher primitives are obtained. These primitives are used to ensure data confidentiality for MIMO–OFDM systems, which will be thoroughly discussed in the following section.

5 Proposed data confidentiality scheme

The proposed data confidentiality scheme consists of two cipher variants. The first cipher variant assumes that frame symbols on different antennas, vary in terms of length. On the other hand, the second variant assumes that all frame symbols contain the same number of modulation symbols. Both schemes are applied after the IFFT transformation (time-domain OFDM frame symbols).

5.1 Case 1: frame symbols of different lengths

The first variant of the proposed solution considers a time-domain frame (F) (after IFFT) that includes n OFDM frame symbols. The length of these frame symbols varies from one antenna to another ($l_1, l_2, l_3, \ldots, l_{nt}$ for antennas $1, 2, \ldots, nt$), as shown in Fig. 3. The elements of each frame symbol on each antenna is randomly circularly shifted based on its corresponding value in π_{nt}. The utilized permutation vector/table has a size of $nt \times 1$ and random values between 1 and nt. For clarification, a simple example is shown in Fig. 3. For the second set of frame symbols (FS_2) on the available antennas, π_{nt} is first updated/permuted using π_{update}, and then employed. This step is repeated n times, that is for each new frame symbol in the frame. Consequently, this complicates the adversary's job and decreases the probability of successful attacks. At the receiver's side, the same steps are performed but using a reversed circular shift operation. It is assumed that $nt \le l_i,\ i = 1,\ 2,\ \ldots,\ nt$.

5.2 Case 2: frame symbols of the same length

The second cipher scheme (variant) is divided into two steps: masking and 2-D permutation.

Following the IFFT transformation (time-domain), each OFDM frame (F) will include n OFDM frame symbols (FS), and each OFDM FS will include l complex modulation symbols. Similar to the first variant, this technique also performs ciphering at the modulation symbol level. More specifically, each frame symbol on each antenna branch is grouped with the rest of the frame symbols on other antennas, forming a set of $nt \times 1$ frame symbols ($nt < n$). This scheme is repeated for all n frame symbols in one frame. Here, every set of nt frame symbols is processed, independently.

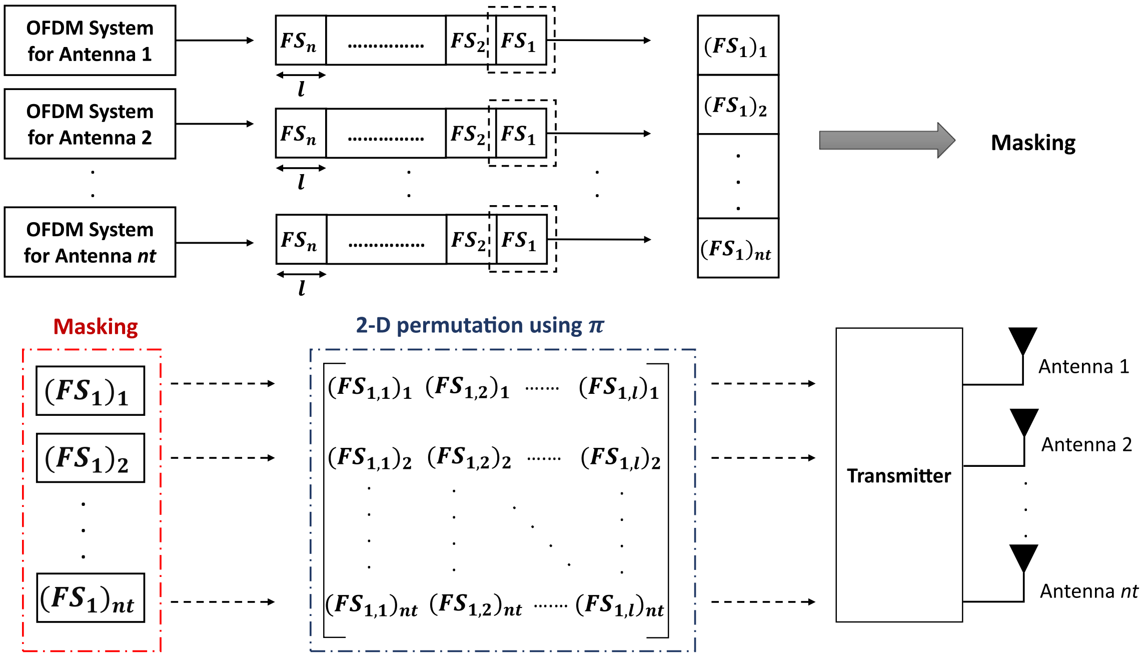


Fig. 5 Proposed data confidentiality scheme: Case 2

- *Masking*: This step handles each FS on each antenna (within the set of nt frame symbols), separately (Fig. 4). In particular, the phases of the real and imaginary components of each complex modulation symbol are modified based on two values in S_1 and S_2, respectively. The sequences S_1 and S_2 have a length of l and contain pseudo-random values of 1 and -1. For the first modulation symbol in the frame symbol, the real component is multiplied by the first value in S_1 and the imaginary component is multiplied by the first value in S_2. Assuming that the first values in S_1 and S_2 are equal to -1 and 1, respectively, then a modulation symbol $a + jb$ will become $-a + jb$. This process is repeated l times, so that all of the modulation symbols within one FS are masked. For every new set of FS (on all antennas), S is updated using CS (cyclic shift). Once all nt frame symbols are masked within one set, 2-D permutation is applied.
- *2-D permutation*: The resulting nt frames symbols are concatenated vertically (grouped) to compose a matrix, in such a way that the values of the first FS represent the first row in the data matrix, D, the values of the second FS represent the second row, and so on. Consequently, the obtained 2-D matrix, D, will have a dimension equal to $nt \times l$ (nt rows and l columns). Next, the permutation table, π, is reshaped and transformed to an $nt \times l$ matrix, which is used to randomly permute D. Matrix, C, which results from the permutation operation, also has nt rows and l columns, similar to D. For each subsequent group of nt frame symbols, π is updated using π_{FS}. The permutation table, π, is also updated using π_F for every new frame.

After the encryption process, each row in matrix C will be transmitted on a different antenna (spatial multiplexing), concurrently. The proposed scheme is shown in Fig. 5.

At the receiver's side, the same steps are performed to decrypt and recover the transmitted data, but, in a reversed order. In addition, inverse cipher primitives are used, which are π^{-1}, π_{FS}^{-1} and π_F^{-1}.

6 Security analysis

In the following, the security level of the two proposed cipher variants is analyzed and assessed.

For this evaluation, several security metrics and tests are presented, which are the randomness degree, recurrence, uniformity and sensitivity. In general, these metrics are commonly-used by researchers to quantify the robustness and effectiveness of conventional upper layer cryptographic algorithms [42]. However, authors in many recent papers have also relied on traditional security criteria to quantify the security of emerging PLS solutions at the physical layer [39,40]. It should be noted that both of the proposed cipher variants achieve the desired security level and have similar performance and test results, hence, we present the results of the second proposed cipher variant, only.

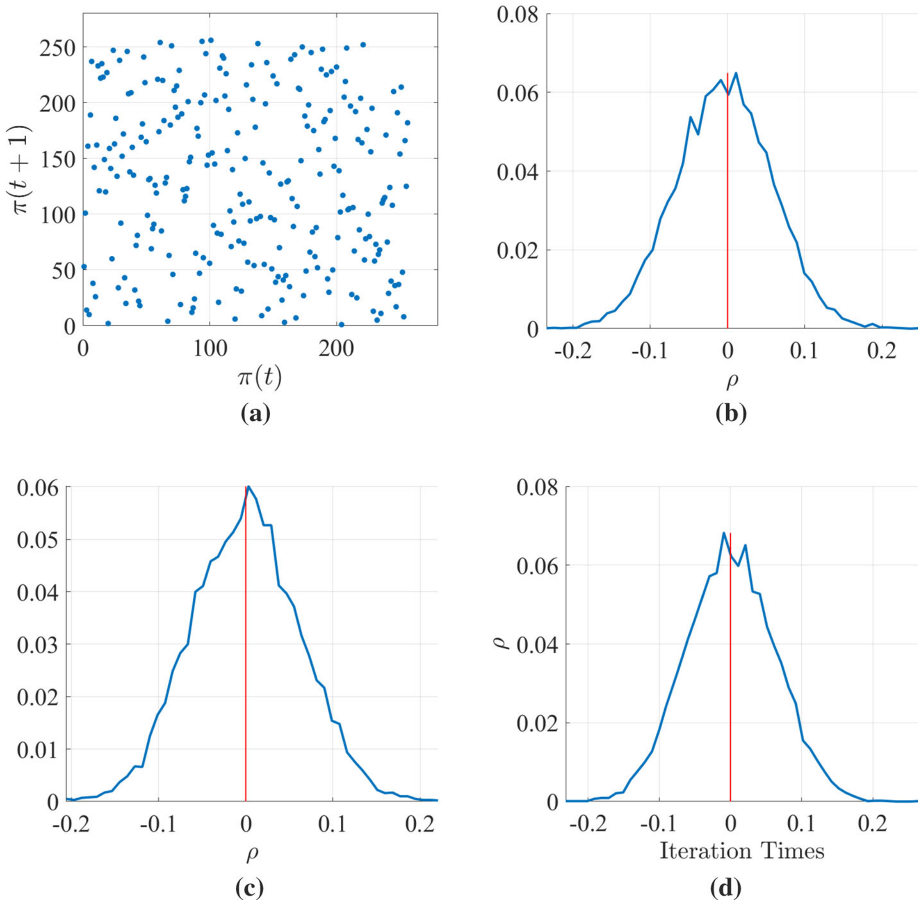


Fig. 6 **a** The recurrence plot of a randomly generated primary permutation table. The probability density function (PDF) (1000 times) of the correlation coefficient (**b**) of multiple primary permutation tables, **c** of the primary permutation table and its updated version (permuted version), and **d** of two successive permutation tables

6.1 Security level of utilized cryrptographic primitive

Both cipher variants mainly depend on the permutation scheme due to its high security level and simplicity (low complexity and overhead). To increase this technique's robustness even further, we have proposed a simple updating method based on permutation to avoid the issue of having a static permutation table throughout the entire communication session.

In order to evaluate the security level of the permutation primitive, we have plotted the recurrence of a primary permutation table in Fig. 6a. From the obtained results, we can prove that this cipher primitive is secure since it has a high randomness degree. In particular, the marked points are uniformly spread all over the available region (randomized). In general, the recurrence plot is a 2D representation that evaluates correlation over time. Using this plot, one can infer whether a system is periodic or chaotic.

Figure 6b shows the distribution (Probability Density Function (PDF)) of the correlation coefficients between several primary permutation tables. From this graph, it is evident that the produced permutation tables are uncorrelated and independent. It has also been shown that a primary permutation table and its updated version are uncorrelated, where most correlation values are close to zero (Fig. 6c). This confirms that the proposed update method is secure and can be employed. Finally, Fig. 6d demonstrates the correlation between any two successive permutation tables. The majority of these values are equal to zero, which is the desired outcome.

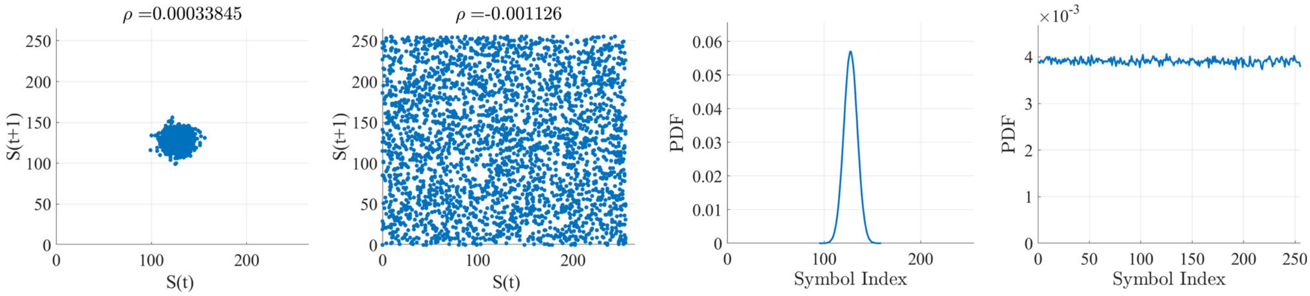
Hence, this confirms the robustness of the permutation primitive and its safe deployment in the proposed cipher variants.

6.2 Randomness degree

The security level of a specific cipher scheme is strongly related to the randomness degree of the encrypted frame symbols. Consequently, we evaluate randomness of the resulting ciphertext using three different tests, which are uniformity, recurrence and independence.

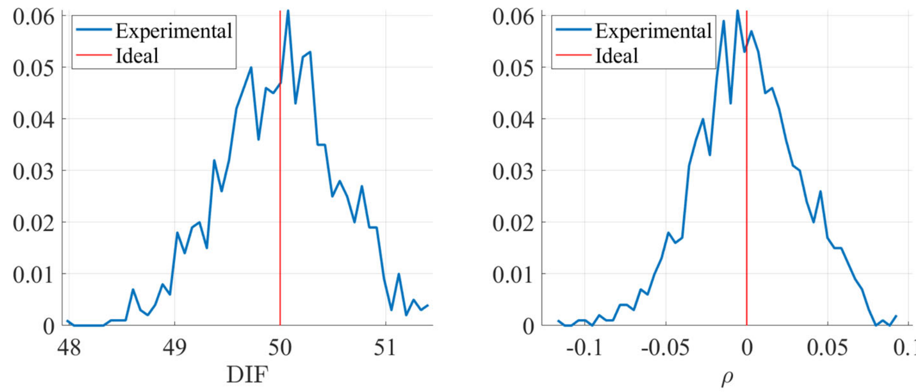
6.2.1 Uniformity

To assess the uniformity property, we have used a simple and straightforward method which is the PDF. First, we have generated normally distributed data with a very low random-



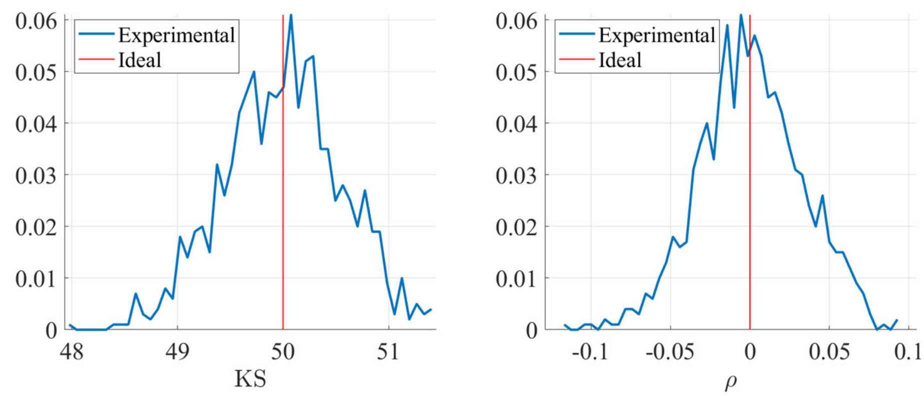
(a) Recurrence of original data **(b)** Recurrence of encrypted data **(c)** PDF of original data **(d)** PDF of encrypted data

Fig. 7 Assessment of the original and encrypted messages in terms of recurrence and PDF



(a) Difference **(b)** Correlation

Fig. 8 Independence test: **a** difference measurements versus the number of transmitted frames. **b** Correlation coefficients between the plaintext and ciphertext



(a) Secret key sensitivity **(b)** Correlation of nonce

Fig. 9 **a** The sensitivity measurements of the secret key versus the number of transmitted frames. **b** Correlation coefficient between the different nonce values

ness degree as depicted in Fig. 7c. In particular, the original data has most of its values centered around a specific value. Next, we have encrypted the original data using the second cipher variant and plotted its distribution. From Fig. 7d, it is clear that the obtained ciphertext has a uniform distribution, where all values have an equal probability of occurrence.

6.2.2 Recurrence

Figure 7a, b represent the recurrence plots of the original and encrypted data, respectively. Unlike the original data which lacks randomness (recurrence points are grouped in one region), the encrypted data has a highly scattered recurrence plot. Therefore, this proves that the proposed scheme achieves the required security level.

6.2.3 Independence

The independence property measures the difference probability between the original frame symbol, FS, and its corresponding encrypted version, $E_K(FS)$, at the bit level. This value should always be close to 0.5 or 50%. The following equation is used to compute the difference value:

$$dif = \frac{\sum_{i=1}^{l} dec2bin(FS) \oplus dec2bin(E_K(FS))}{l}, \quad (3)$$

where K is the utilized encryption key. Indeed, the obtained results in Fig. 8a prove that the proposed cipher variant attains the independence property, in which the majority of the difference values are equal to the ideal value, 50%.

Additionally, we have calculated the correlation between the plaintext and ciphertext. As shown in Fig. 8b, the correlation coefficients have a normal distribution centered around the desired value, 0.

6.3 Key sensitivity

This test measures the bit-difference in encrypted frame symbols when using slightly different keys (one-bit change). The difference value between the ciphered frames should always be near 0.5 or 50% (at the bit level). In principle, the sensitivity of a key, K, is calculated as follows:

$$KS = \frac{\sum_{i=1}^{l} dec2bin(E_K(FS)) \oplus dec2bin(E_{K'}(FS))}{l}. \quad (4)$$

Here, all of the elements of K and K' are identical, except for the Least Significant Bit (LSB) of a random byte. Moreover, both of the original and ciphered frame symbols have a length equal to l (in bits).

Figure 9a proves that the key sensitivity property is achieved using the proposed solution, since the key sensitivity values are close to 50%. Finally, Fig. 9b shows that different nonce values are independent and uncorrelated.

6.4 Plaintext sensitivity

The plaintext sensitivity test utilizes a key, K, to encrypt two frame symbols (FS and FS'), that differ by only one bit. Then, it computes the difference in the output bits. This difference should be at least 0.5 or 50% (in bits). Plaintext sensitivity is evaluated according to:

$$PS = \frac{\sum_{i=1}^{l} dec2bin(E_K(FS)) \oplus dec2bin(E_K(FS'))}{l}, \quad (5)$$

where K is the encryption key and l is the length of the frame symbols.

For the proposed cipher variants in this paper, the plaintext sensitivity is omitted since a dynamic update process is performed. More specifically, different dynamic keys are generated for every new session and different cipher primitives are derived for every input frame and/or set of frame symbols (depends on configuration). In this way, one can guarantee that the proposed cipher schemes ensure the avalanche effect by producing completely different and independent encrypted frames.

It should be noted that the first cipher variant achieves a similar security performance as the second variant, hence, its test results have been omitted.

7 Cryptanalysis

In order to validate the security and robustness of the two proposed cipher variants, we discuss and analyze these schemes in the context of different attacks, namely, statistical attacks, differential attacks, brute force attacks and related key attacks.

Here, it is assumed that the adversary has full knowledge regarding: the protocols used for transmission, the proposed cipher algorithm (known publicly), the encrypted frames that are exchanged between the transmitter and receiver, the shared wireless channel and its characteristics. On the other hand, the adversary does not have the secret key.

7.1 Statistical attacks

To ensure high resilience against this type of attacks, a security scheme should produce ciphertext with a high degree of randomness. Based on the security tests presented in the previous section, both of the proposed cipher schemes have been proven to be secure and suitable for implementation in current and future systems. More specifically, results have shown that encrypted symbols are uniformly distributed and have highly dispersed recurrence plots. The proposed schemes also achieve the independence property, since the bit-difference between the input data and the corresponding ciphertext is always close to the desired value, 50% (at least 50%). Consequently, the requirements needed to resist statistical attacks, are successfully attained.

7.2 Linear and differential attacks

In linear/differential attacks, adversaries exploit the relationship between two encrypted OFDM symbols, in an attempt to acquire the used cipher primitives, encryption keys or any useful information. To overcome this issue, we have proposed a dynamic update process, that changes/updates the cipher primitives for every nt frame symbols or every OFDM frame. The update process, mainly, depends on the simple and lightweight permutation technique, which randomly shuffles the utilized cipher primitives, in an efficient manner. Hence, the produced ciphertext are uncorrelated, random and independent. This has also been validated using the key sensitivity test. More specifically, results have revealed that an OFDM frame symbol, encrypted using two different keys, results in two frame symbols, having at least 50% of their bits different. As a result, no valuable information can be learnt from ciphered data, hence, linear and differential attacks are ineffective in this case.

The proposed schemes are also secure against chosen/known plaintext/ciphertext attacks, which are a sub-set of linear and differential attacks.

7.3 Brute force attacks

In both cipher schemes, the pre-shared secret key can have a length of 128, 196, or 256 bits. Based on the size of the secret key, the size of the channel-derived nonce is adjusted accordingly (padding), since both, the nonce and the secret key, should have the same size in order to perform the XOR operation. On the other hand, the size of the generated dynamic key is 512 bits, since the SHA-512 hash function is utilized. This key-size is acceptable for preventing brute force attacks.

7.4 Related key attacks and weak keys

From the key sensitivity test, it is evident that the desired key sensitivity probability (0.5 or 50%) is achieved, hence, both proposed schemes are able to resist any related-key attack. In both variants, a dynamic key is generated from a channel-based parameter, which is referred to as a nonce and a secret key. This key is, then, fragmented into a number of smaller sub-keys, each used to derive a specific cipher primitive. Acquiring the dynamic key or sub-keys is rather a hard task for illegitimate users, since they should be able to, correctly, estimate the physical channel between communicating devices and extract the same channel-based information. To increase the security of the proposed key generation function, a secret key is combined with the channel-based nonce to decrease the probability of successfully deriving the dynamic key and the cipher primitives. The secret key is only known to the legitimate users.

Unlike symmetric and upper layer cipher schemes which consist of static cipher primitives, the proposed solution updates the utilized cipher-primitives, frequently and dynamically. Therefore, the obtained frame symbols are independent and uncorrelated. In particular, one permutation table (π_{nt}) and one update permutation table (π_{update}) are generated for the first cipher variant, and one permutation table (π), one masking sequence (S) and three update permutation tables (vectors) are produced in the second case (π_{FS}, π_F and CS). These cryptographic primitives change for each new input frame symbol. Such an approach complicates the process of recovering transmitted data, correctly. Any vulnerability in any of the dynamic keys will not affect the previously processed or the following data frames symbols. Thus, the proposed solution is also resilient to weak keys.

8 Performance analysis

In this section, the proposed cipher variants are evaluated in terms of error propagation and execution time. These criteria are crucial for assessing the performance and efficiency of any cipher approach. Generally, an efficient PLS-based cipher scheme should have low latency/delay (execution time) and low error propagation. For the proposed schemes, this can be easily verified since a one-round cipher structure that consists of two simple operations is employed (phase modification and permutation).

8.1 Error propagation

Both of the proposed schemes require a single round and depend on simple operations to secure the data conveyed in MIMO–OFDM systems. In particular, the proposed ciphering process is applied at the lowest layer, which is the physical layer, using random and dynamic parameters extracted from the physical channel itself. Using these parameters and a secret key, users generate a dynamic key and derive the needed cryptographic primitives. Both schemes mainly depend on permutation which is a simple, efficient and robust security technique. This scheme avoids the diffusion operation which one of the main causes of error propagation in communication systems. Moreover, the shuffling/permutation operation does not result in the spread of error among bits, where error is restricted to one position, only. Consequently, the proposed schemes do not affect the bit error rate, and do not cause degradation in performance. This makes them good security candidates for emerging communication systems and technologies. It should also be noted that the proposed schemes are applied at the frame symbol level, that is on modulation symbols, hence, error does not propagate to other frame symbols in the frame.

8.2 Computational complexity and execution time

Traditional block cipher approaches introduce a large cost in terms of computations and resources [42]. Recently, researchers have shown interest in designing new cryptographic algorithms structures that require low overhead in terms of latency and resources.

Several lightweight ciphers have been presented in the ongoing effort to address the computational complexity issue using simple functions with simple operations, including LED (PHOTON family) [43,44], Simon and Speck [45]. However, these algorithms preserve the multi-round struc-

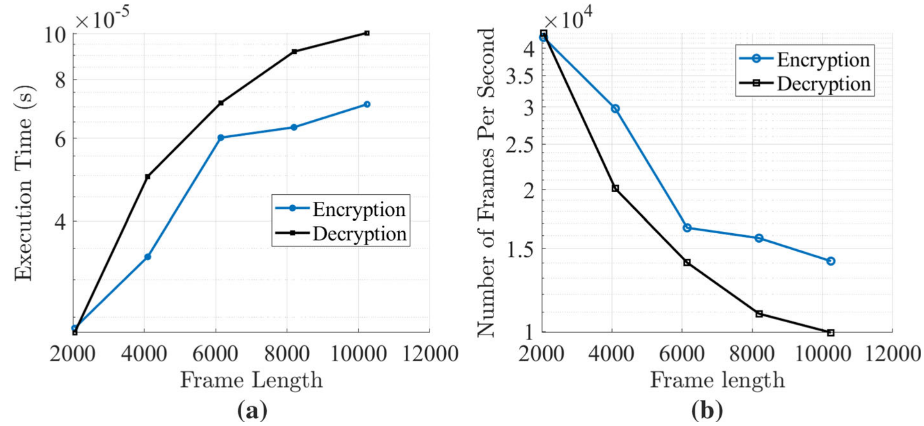


Fig. 10 **a** Execution time in seconds versus frame size using the proposed cipher scheme on one antenna. **b** Number of encrypted frame versus frame length

ture. On the contrary, the proposed solution uses a lightweight function with one round and one operation.

Next, we evaluate the computational delays of the proposed cipher schemes. The main goal of the proposed schemes is to ensure robust security with minimal overhead (number of operations and iteration rounds). For the derivation of the computational delay, we define the following parameters:

(1) r_o represents the number of encryption/decryption rounds.
(2) Sb_t denotes the execution time of the substitution operation for an input block of 16 bytes.
(3) MC_t represents the delay required by the AES diffusion mix-column operation (for all 4 columns). This operation exhibits the highest delay compared to other AES operations.
(4) XOR_t denotes the logical "Exclusive-OR" execution time.
(5) SR_t represents the delay required by the AES "shift-rows" operation.
(6) h_t is the time required by the hash function.
(7) CCP_t is the time to construct the required cryptographic primitives.
(8) π_t denotes the time required by the permutation operation (this also represents the update operation).
(9) CS_t denotes the time required by the circular shift operation.
(10) MK_t denotes the time required by the masking operation.

To assess the performance of the proposed schemes, we compare with the widely used AES (Advanced Encryption Standard) scheme. Hence, we first calculate the total computation delay of AES [46]:

$$CD_{AES} = r_o Sb_t + (r_o + 1) XOR_t + (r_o - 1) MC_t + r_o SR_t, \quad (6)$$

where r_o is the number of rounds in AES and which has a minimum value of 10 for a 128-bit secret key. In this case, the computational delay of AES becomes:

$$CD_{AES(r_o=10)} = 10Sb_t + 11xor_t + 9MC_t + 10SR_t. \quad (7)$$

Concerning the computational delays of the proposed schemes, we start by the time needed for the key generation technique:

$$CD_{(key.gen)} = 2h_t + XOR_t + CCP_t, \quad (8)$$

The computational delay of the proposed encryption processes (for each frame symbol) is presented by the following equations:

$$CD_{(case1)} = CS_t + \pi_t, \quad (9)$$
$$CD_{(case2)} = MK_t + CS_t + 2\pi_t. \quad (10)$$

It is clear that both cipher variants require fewer operations than the traditional AES scheme, and thus, lower computational complexity and associated delay. This is not surprising since AES requires multiple rounds.

Moreover, note that the first variant exhibits a lower execution time as compared to the second one. Hardware optimization mechanisms can also be leveraged for the permutation process to reduce further the required latency and resources.

Regardless of any optimization, the proposed cipher schemes require fewer rounds and operations as compared to existing standard ciphers that are based on the concept of multi-rounds and multi-operations. This significant reduction is possible due to the dynamic cryptographic concept, which benefits from the dynamic channel parameters; hence, the ability for just a single round.

Moreover, the computational complexity of the proposed schemes is linear ($O(l)$), where l is the number of modulation symbols in each frame symbol.

Figure 10a shows the execution time in seconds versus the input frame size. This simulation is done using MATLAB, and for one antenna only. The execution time on other antennas is also similar since the same operations are carried out on all antennas. As it can be inferred, the proposed solutions are efficient since they introduce low overhead and acceptable execution time, in the order of microseconds. Figure 10b validates the results of Fig. 10a since as the frame length increases, more time is required for execution and less encrypted frames are generated per second. From these figures, it is clear that the decryption process has a higher execution time than the encryption process. This is logical since the decryption process requires the generating of the inverse cryptographic primitives such as the inverse permutation tables.

9 Conclusion

This paper proposes an efficient cipher solution for wireless MIMO–OFDM systems. The proposed solution is comprised of two cipher variants, both of which target the data confidentiality of transmitted data. Particularly, legitimate users exploit the random and dynamic nature of wireless physical channels, to generate simple and lightweight cipher primitives and update cipher primitives. These primitives are updated frequently to minimize the risk of any security threat or vulnerability. The proposed cipher schemes are simple and efficient since both depend on lightweight operations, mainly addition and permutation. Finally, several security and performance tests have been conducted and the results have validated the high security level and efficiency of the proposed cipher schemes.

Funding This research is supported by the Maroun Semaan Faculty of Engineering and Architecture at the American University of Beirut and by the EIPHI Graduate School (contract "ANR-17-EURE-0002").

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Sharma, V., & Kaur, H. (2016). On BER evaluation of MIMO–OFDM incorporated wireless system. *Optik-International Journal for Light and Electron Optics, 127*(1), 203–205.
2. Melki, R., Noura, H., Mansour, M., & Chehab, A. (2019). A survey on OFDM physical layer security. *Physical Communication, 32*, 1–30.
3. Hamamreh, J. M., Furqan, H. M., & Arslan, H. (2018). Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 21*(2), 1773–1828.
4. Tsoulos, G. (2006). *MIMO system technology for wireless communications*. CRC Press.
5. Sivakrishna, S., & Yarrabothu, R. (2018). Design and simulation of 5G massive MIMO kernel algorithm on SIMD vector processor. In *Conference on signal processing and communication engineering systems (SPACES)* (pp. 53–57). IEEE.
6. Melki, R., Noura, H., Mansour, M., & Chehab, A. (2020). Physical layer security schemes for MIMO systems: An overview. *Wireless Networks, 26*(3), 2089–2111.
7. Kapetanovicn, D., Zheng, G., & Rusek, F. (2015). Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Communications Magazine, 53*(6), 21–27.
8. Chen, X., Lei, L., Zhang, H., & Yuen, C. (2015). Large-scale MIMO relaying techniques for physical layer security: AF or DF? *IEEE Transactions on Wireless Communications, 14*(9), 5135–5146.
9. Deng, Y., Wang, L., Wong, K. K., Nallanathan, A., Elkashlan, M., & Lambotharan, S. (2015). Safeguarding massive MIMO aided hetnets using physical layer security. In *International conference on wireless communications signal processing (WCSP)* (pp. 1–5).
10. Yang, Q., Wang, H., Zhang, Y., & Han, Z. (2016). Physical layer security in MIMO backscatter wireless systems. *IEEE Transactions on Wireless Communications, 15*(11), 7547–7560.
11. Schulz, M., Loch, A., & Hollick, M. (2014). Practical known-plaintext attacks against physical layer security in wireless MIMO systems. In *NDSS*
12. Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., & Di Renzo, M. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine, 53*(4), 20–27.
13. Chen, X., Zhong, C., Yuen, C., & Chen, H. H. (2015). Multi-antenna relay aided wireless physical layer security. *IEEE Communications Magazine, 53*(12), 40–46.
14. Poor, H., & Schaefer, R. (2017). Wireless physical layer security. *Proceedings of the National Academy of Sciences, 114*(1), 19–26.
15. Maharaja, N., Mishra, B., & Bansode, R. (2016). Performance evaluation of spatial multiplexing MIMO–OFDM system using MMSE detection under frequency selective Rayleigh channel. *Global Journal of Computer Science and Technology, 15*, 27–33.
16. Omri, A., & Bouallegue, R. (2011). New transmission scheme for MIMO–OFDM. *International Journal of Next Generation Network, 3*(1), 11–19.
17. Lee, Y., Jo, H., Ko, Y., & Choi, J. (2017). Secure index and data symbol modulation for OFDM-IM. *IEEE Access, 5*, 24959–24974.
18. Hamamreh, J. M., Basar, E., & Arslan, H. (2017). OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services. *IEEE Access, 5*, 25863–25875.
19. Zhang, J., Marshall, A., Woods, R., & Duong, T. (2017). Design of an OFDM physical layer encryption scheme. *IEEE Transactions on Vehicular Technology, 66*(3), 2114–2127.
20. Hamamreh, J. M., & Arslan, H. (2017). Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond. *IEEE Communications Letters, 21*(5), 1191–1194.
21. Cheng, D., Gao, Z., Liu, F., & Liao, X. (2015). A general time-domain artificial noise design for OFDM AF relay systems. In *Proceedings of IEEE/CIC international conference on communications in China (ICCC), Shenzhen, China, November* (pp. 1–6).
22. Akitaya, T., & Saba, T. (2015). Energy efficient artificial fast fading for MISO–OFDM systems. In *Proceedings of IEEE global*

communications conference (GLOBECOM), San Diego, CA, USA, December (pp. 1–6).
23. Rahbari, H., & Krunz, M. (2017). Exploiting frame preamble waveforms to support new physical-layer functions in OFDM-based 802.11 systems. *IEEE Transactions on Wireless Communications, 16*(6), 3775–3786.
24. Zhang, W., Zhang, C., Chen, C., Jin, W., & Qiu, K. (2016). Joint PAPR reduction and physical layer security enhancement in OFDMA-PON. *IEEE Photonics Technology Letters, 28*(9), 998–1001.
25. Xiao, Y., Chen, M., Li, F., Tang, J., Liu, Y., & Chen, L. (2015). PAPR reduction based on chaos combined with SLM technique in optical OFDM IM/DD system. *Optical Fiber Technology, 21*, 81–86.
26. Lim, D., No, J., Lim, C., & Chung, H. (2005). A new SLM OFDM scheme with low complexity for PAPR reduction. *IEEE Signal Processing Letters, 12*(2), 93–96.
27. Tsai, Y., Tai, C., Yang, K. (2014). Effective channel perturbation based on cyclic delay for physical layer security in OFDM systems. In *Proceedings of international conference on information science, electronics and electrical engineering (ISEEE), Sapporo, Japan, April 2014* (Vol. 2, pp. 823–827).
28. Hamamreh, J. M., Furqan, H., & Arslan, H. (2017). Secure precoding and post-coding for OFDM systems along with hardware implementation. In *Proceedings of IEEE international wireless communications and mobile computing conference (IWCMC), Valencia, Spain, June 2017* (pp. 1338–1343).
29. Li, H., Wang, X., & Zou, Y. (2014). Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems. *IEEE Communications Letters, 18*(6), 1059–1062.
30. Zhang, B., Zhan, Q., Chen, S., Li, M., Ren, K., Wang, C., & Ma, D. (2014). Priwhisper: Enabling keyless secure acoustic communication for smartphones. *IEEE Internet Of Things Journal, 1*(1), 33–45.
31. Huo, F., & Gong, G. (2014). A new efficient physical layer OFDM encryption scheme. In *Proceedings of IEEE international conference on computer communications (INFOCOM), Toronto, ON, Canada, April 2014* (pp. 1024–1032).
32. Wang, Y., & Zhang, L. (2017). High security orthogonal factorized channel scrambling scheme with location information embedded for MIMO-based VLC system. In *2017 IEEE 85th vehicular technology conference (VTC Spring), June 2017* (pp. 1–5).
33. Tanigawa, Y., Kozai, Y., & Saba, T. (2017). A physical layer security scheme employing imaginary receiver for multiuser MIMO–OFDM systems. In *Proceedings of IEEE international conference on communications (ICC), May 2017* (pp. 1–6).
34. Ahmed, M., & Bai, L. (2017). Space time block coding aided physical layer security in Gaussian MIMO channels. In *International Bhurban conference on applied sciences and technology (IBCAST), January 2017* (pp. 805–808).
35. Chen, X., & Zhang, Y. (2017). Mode selection in MU-MIMO downlink networks: A physical-layer security perspective. *IEEE Systems Journal, 11*(2), 1128–1136.
36. Zhang, Y., Liang, T., & Sun, A. (2015). Joint transmit antenna selection and jamming for security enhancement in MIMO wiretap channels. In *IEEE proceedings of international conference on communications, China (ICCC), November 2015* (pp. 1–6).
37. Li, G., & Hu, A. (2016). Virtual MIMO-based cooperative beamforming and jamming scheme for the clustered wireless sensor network security. In *IEEE proceedings of international conference on communications, China (ICCC), October 2016* (pp. 2246–2250).
38. Fan, Y., Liao, X., & Vasilakos, A. V. (2017). Physical layer security based on interference alignment in K-User MIMO Y wiretap channels. *IEEE Access, 5*, 5747–5759.
39. Melki, R., Noura, H. N., Mansour, M. M., & Chehab, A. (2018). An efficient OFDM-based encryption scheme using a dynamic key approach. *IEEE Internet of Things Journal, 6*, 361–378.
40. Noura, H., Melki, R., Chehab, A., & Mansour, M. M. (2018). A physical encryption scheme for low-power wireless M2M devices: A dynamic key approach. *Mobile Networks and Applications, 24*, 1–17.
41. Noura, H., Melki, R., Chehab, A., Mansour, M. M., & Martin, S. (2018). Efficient and secure physical encryption scheme for low-power wireless M2M devices. In *IWCMC security symposium, Limassol, Cyprus, June*.
42. Noura, H., Chehab, A., Sleem, L., Noura, M., Couturier, R., & Mansour, M. M. (2018). One round cipher algorithm for multimedia IoT devices. *Multimedia Tools and Applications, 77*(14), 18383–18413.
43. Guo, J., Peyrin, T., & Poschmann, A. (2011). The photon family of lightweight hash functions. In *Annual cryptology conference* (pp. 222–239). Springer.
44. Guo, J., Peyrin, T., Poschmann, A., & Robshaw, M. (2011). The led block cipher. In *International workshop on cryptographic hardware and embedded systems* (pp. 326–341). Springer.
45. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). Simon and speck: Block ciphers for the internet of things. *IACR Cryptology ePrint Archive, 2015*, 585.
46. Heron, S. (2009). Advanced encryption standard (AES). *Network Security, 2009*(12), 8–12.

Reem Melki received her BS degree in electrical and computer engineering from the Rafik Hariri University in 2013, and her MS degree in 2015. She is currently a Ph.D. student at the American University of Beirut (AUB). Her main areas of research interests include security and privacy in wireless and mobile communication.

Hassan Noura received his degree in Computer and Communication Engineering from the IUL University in 2008, Lebanon, and his Ph.D. degree from Polytech'Nantes in 2012, France. In 2013, Noura joined Paris-Sud XI University, as a postdoctoral researcher, after that as research engineering at CEA, Grenoble. After that, he joined QMIC in 2015 and Telecom ParisTech in 2016. Recently, he gets his HDR in 2016 and joins AUB in 2017 as lecturer in the ECE Department. In 2021, he became Full Professor at the University of Bourgogne

Franche-Comté, computer science department. His research interests include cryptography, network security, secure network coding, multimedia and distributed system.

Ali Chehab received his Bachelor degree in EE from AUB in 1987, the Master's degree in EE from Syracuse University in 1989, and the PhD degree in ECE from the University of North Carolina at Charlotte, in 2002. From 1989 to 1998, he was a lecturer in the ECE Department at AUB. He rejoined the ECE Department at AUB as an Assistant Professor in 2002, became Full Professor in 2014. He received the AUB Teaching Excellence Award in 2007. He teaches courses in Programming, Electronics, Digital Systems Design, Computer Organization, Cryptography, and Digital Systems Testing. His research interests include: Wireless Communications Security, Cloud Computing Security, Multimedia Security, Trust in Distributed Computing, Low Energy VLSI Design, and VLSI Testing. He has about 210 publications. He is a senior member of IEEE and a senior member of ACM.