Efficient data confidentiality scheme for 5G wireless NOMA communications

Hassan Noura, Reem Melki, Ali Chehab

Efficient Data Confidentiality Scheme For 5G Wireless NOMA Communications

Hassan N. Noura[1], Reem Melki[2], and Ali Chehab[2]

[1]Univ. Bourgogne Franche-Comté (UBFC), FEMTO-ST Institute, CNRS, Belfort, France
[2]Department of Electrical and Computer Engineering, American University of Beirut, Lebanon, Emails: {hn49,rmm71, chehab}@aub.edu.lb

November 29, 2021

Abstract

Non-Orthogonal Multiple Access (NOMA) has recently emerged as a promising multiple access technique for current and future mobile communication networks. Unlike conventional multiple access schemes, NOMA exploits the power domain to service a large number of users at different power levels, using the same time-frequency resources. However, this technology suffers from major security threats since users are able to decode the messages of other paired users utilizing the same resources. In this paper, we propose an efficient and lightweight cipher scheme for NOMA systems at the physical layer. Unlike previous schemes in the literature, the proposed solution combines cryptography and Physical Layer Security (PLS) to provide robust security at minimum cost by adopting a structure that requires a single round with a single operation. Moreover, it is generic in the sense that any simple cipher operation such as permutation, substitution, phase shuffling, or pseudo-random masking, can be utilized in order to secure the underlying NOMA frame symbols. Also, we propose a dynamic key derivation scheme that benefits from the dynamic properties of wireless channels. Simulation results and cryptanalysis show that the proposed solution achieves the desired security level and strikes a good balance between performance and security level.

Keywords— Non-Orthogonal Multiple Access; physical layer security; cryptanalysis; security analysis; wireless networks; dynamic key.

1 Introduction

Multiple Access (MA) is a technique that allows mobile users to 1) establish wireless connections with different networks, and 2) share the available resources, namely, the allotted spectrum, in

an effective and efficient manner. Particularly, MA improves the overall capacity within a specific geographical area since various terminals are able to transmit data using the same bandwidth, simultaneously [1, 2]. Over the past few years, several MA technologies have been developed such as Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), and Orthogonal Frequency Division Multiple Access (OFDMA). These multiple access technologies have gained a lot of popularity and led to the evolution of wireless systems from the first generation (1G) to the fourth generation (4G), where different signals are mapped onto orthogonal resources in either the frequency domain, time domain, code domain or time-frequency domain [3].

With the birth of the fifth generation wireless communication systems (5G), new challenges have risen for conventional Orthogonal Multiple Access (OMA) techniques such as super-high data rates, ultra-low latency, ultra-reliability and massive connectivity. These new requirements should be met in order to realize the full potential of future wireless systems. As a result, Non-Orthogonal Multiple Access (NOMA) has emerged as a promising candidate to overcome the current limitations and fulfill such requirements. Using this method, the signals of different users can be transmitted over the same time-frequency resources, concurrently [1, 4]. In order to distinguish the multiplexed signals, either the power domain or code domain is used for multiple access.

Potential applications of NOMA include mobile communication, vehicular communication and Internet-of-Things (IoT) ecosystems. Traditional Radio Frequency (RF) communication systems suffer from high interference, large delays, extreme congestion of radio spectrum, in addition to many security vulnerabilities. NOMA, on the other hand, overcomes these issues since it is immune to electromagnetic interference and has a large bandwidth. However, this technology is not fully immune against all types of attacks and security vulnerabilities. Consequently, improving the confidentiality of transmitted data is an inevitable requirement to ensure secure and robust communication between entities [5, 6].

In this paper, a robust and lightweight cipher scheme is proposed for PD-NOMA downlink systems to enhance data confidentiality, efficiently. The importance of the proposed solution is that it combines the dynamicity of wireless channels with traditional cryptography, to define a novel and secure dynamic cipher scheme at the physical layer. The proposed solution is simple and efficient since it only requires a single round. It is also generic since any cryptographic operation can be employed such as permutation, substitution, phase modification, or masking [7]. A dynamic key generation approach is also presented and it is based on the common channel characteristics and physical parameters (pseudo-random and dynamic) between the Base Station (BS) and mobile users. The dynamic key is used to generate cipher primitives and their corresponding update primitives. The update primitives are used to change the cipher primitives for every input symbol or frame in order to further increase the security level. The proposed scheme exhibits a high security level against passive attacks while maintaining low computational complexity. The results of performance assessment confirm the efficiency of the proposed solution in terms of latency, required resources, and error propagation (effect of channel and fading). On the other hand, the results of security tests validate the security level and robustness of the proposed approach.

The rest of the paper is organized as follows. Section 2 overviews the types of NOMA and the corresponding system model. Section 3 briefly discusses the related work in the literature. Section 4 describes in details the proposed cipher scheme. Section 5 presents the experimental security analysis. Section 6 includes a detailed cryptanalysis discussion. Section 7 evaluates the performance of the scheme. Finally, Section 8 concludes the paper.

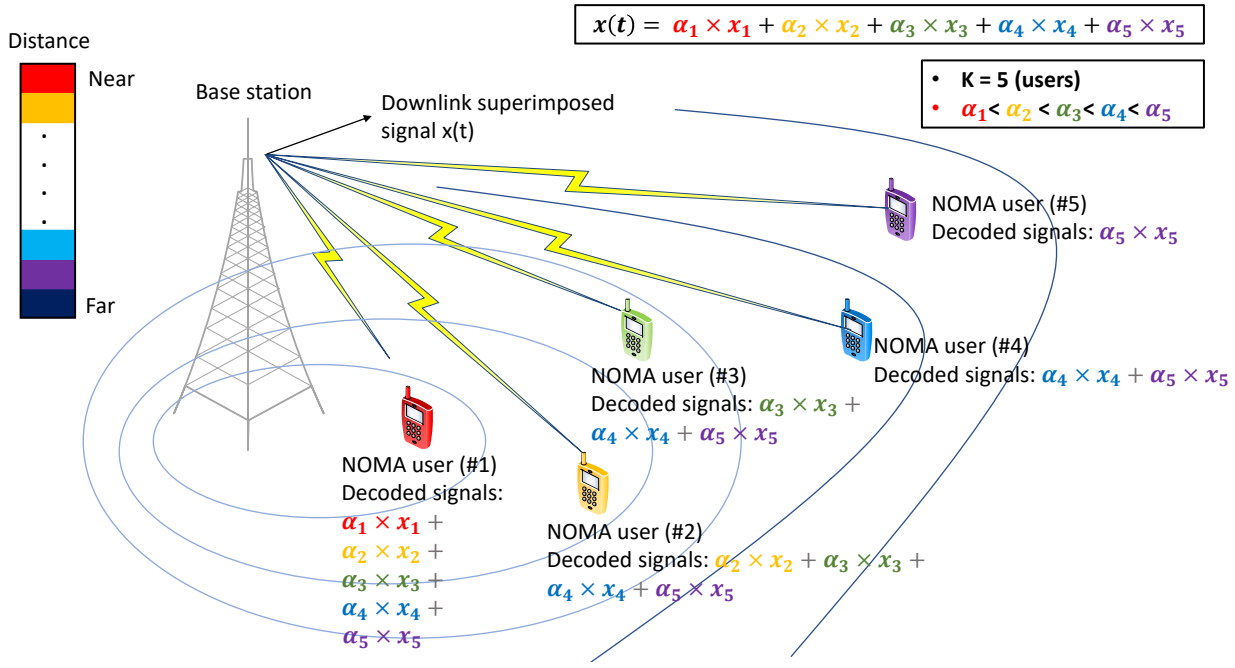


Figure 1: NOMA downlink system with five NOMA users

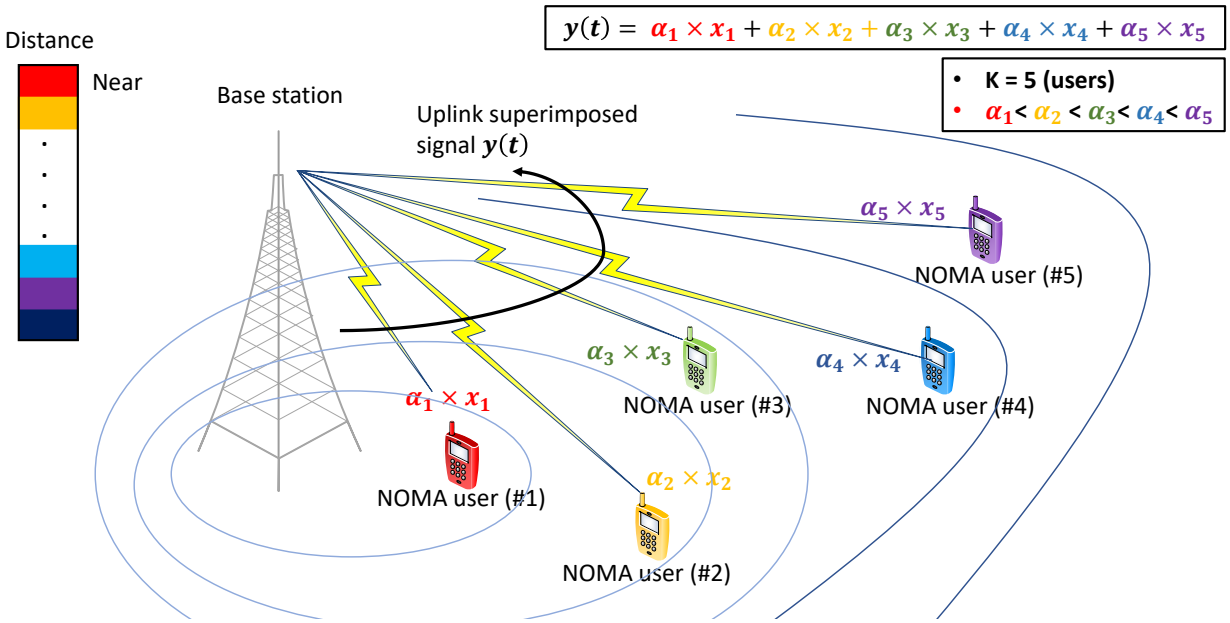


Figure 2: NOMA uplink system with five NOMA users

2 Background

In this section, we present the necessary background information related to the NOMA technology. Table 1 lists the notations used in this paper.

Table 1: Table of notations

Notation	Definition
SK	Common secret key
Ch	Channel gain
D_i	i^{th} device in the cell
K	Number of devices in a cell
DK	Dynamic key
P_{BS}	Total power at the base station
$x_i(t)$	Plaintext signal of user i
$x_i'(t)$	The received downlink signal at user i
$x(t)$	Superimposed downlink signal from the base station
$y(t)$	Uplink signal from users to base station
$c_i(t)$	Encrypted signal of user i
α_i	Power coefficient of user i
N	Number of symbols in one frame
$n(t)$	Additive white Guassian noise
FS	Frame symbol
EFS	Encrypted frame symbol
$h(\cdot)$	Hash function
$(\cdot)^T$	Transpose operation
$\oplus$	Exclusive-OR (XOR)
π	Update permutation table
m	Number of bits in one frame symbol
$\|\|$	Concatenation

2.1 Types of NOMA

In general, NOMA schemes are divided into two main classes: Power-Domain NOMA (PD-NOMA) [8] and Code-Domain NOMA (CD-NOMA) [9]. In the former case, different users, sharing the same time-frequency resources, are assigned different power coefficients based on their channel conditions [10]. Following the allocation of power coefficients, the resulting signals are superimposed and transmitted as shown in Fig. 1. At the receiver, Successive Interference Cancellation (SIC) is used to decode the signals, one by one, until the desired signal is obtained [11].

In CD-NOMA, different signals are also multiplexed over the same time-frequency resources, however, using unique codes. Specifically, each user is allocated a unique non-orthogonal code, with low cross-correlation or sparse sequences [9]. Examples of CD-NOMA include Multi-User Shared Access (MUSA), Sparse Code Multiple Access (SCMA), and Low-Density Spreading (LDS). The concept of CD-NOMA is similar to that of Code Division Multiple Access (CDMA), expect for the fact that CDMA utilizes orthogonal codes [12]. There are other less popular NOMA schemes such as Pattern Division Multiple Access (PDMA) and Bit Division Multiplexing (BDM).

Currently, more attention is being directed towards PD-NOMA than CD-NOMA due to its simplicity, efficiency and applicability to current systems. Moreover, no additional bandwidth nor major changes are required to improve spectral efficiency. Therefore, we focus in this paper on PD-NOMA, and which we refer to as NOMA for simplicity.

2.2 NOMA System Model

The system model of NOMA includes downlink NOMA and uplink NOMA.

2.2.1 Downlink NOMA Network

In the downlink case, the Base Station (BS) superimposes all of the devices' information signals into a single waveform using different power coefficients; the device that is farthest from the BS is allocated maximum power, while the nearest device is allocated minimum power. Power allocation is also related to the quality of the channel and its conditions. All users in the network receive the same signal, which contains the information of all devices. For the recovery of individual signals, each device performs SIC to decode the strongest signal, and then subtracts it from the received signal. This operation is iterated successively until the device finds its own signal. In contrast, the Far User, which has the highest power coefficient, is able to recover its desired signal directly without performing SIC, since other signals are treated as noise [13]. The transmitted signal ($x(t)$) can be written as:

$$x(t) = \sum_{i=1}^{K} \sqrt{\alpha_i P_{BS}} x_i(t), \tag{1}$$

where $x_k(t)$ is the individual information of device i, P_{BS} is the transmission power at the BS, K is the number of users in the network, and α_i is the power allocation coefficient for user i. The received signal ($x_i'(t)$) at i^{th} user is expressed as follows:

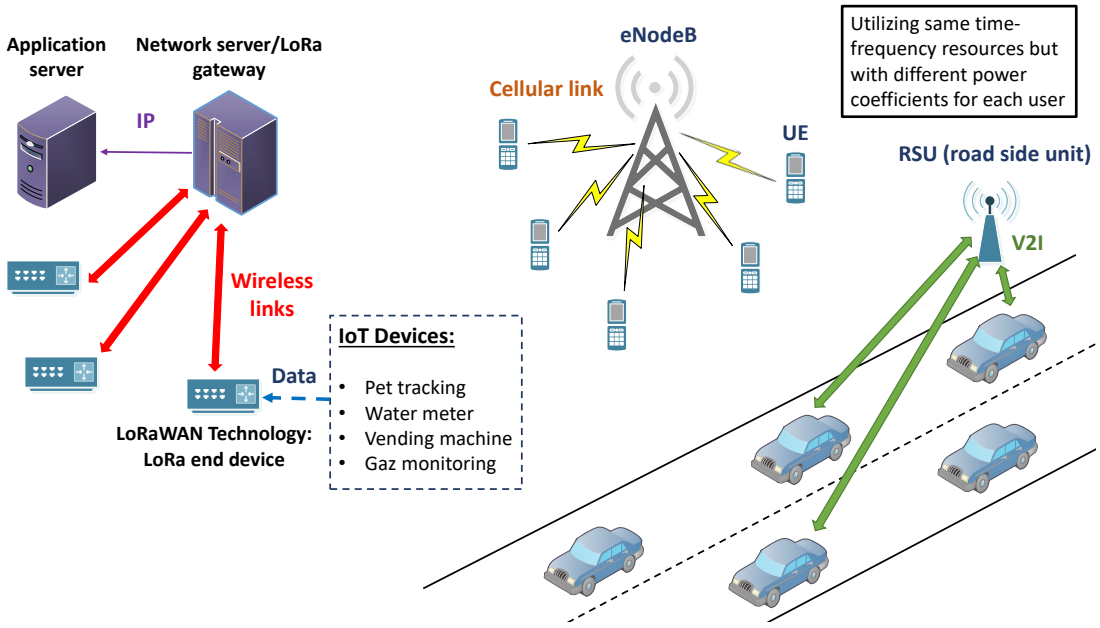


Figure 3: Applications of NOMA

$$x_i'(t) = Ch_i x(t) + n_i(t) = Ch_i \sum_{i=1}^{K} \sqrt{\alpha_i P_{BS}} x_i(t) + n_i(t), \tag{2}$$

where Ch_i is the channel coefficient of the i^{th} user, and $n_i(t)$ is the additive white Gaussian noise at the i^{th} device with a mean of zero and density N_0.

2.2.2 Uplink NOMA Network

In the uplink NOMA network, each user transmits its signal to the BS (Fig. 2). The signals are multiplexed into one signal, and at the BS, SIC is applied to detect and distinguish the signal of each user [13]. The received signal at the BS, which includes the signals of all users, is represented as follows:

$$y(t) = \sum_{i=1}^{K} Ch_i x_i(t) + n_i(t). \tag{3}$$

Here, devices optimize their transmit powers according to their locations, as in the downlink case.

This system model is suited for Single-Input Single-Output (SISO) systems, where channels are represented by scalars. Similarly, NOMA can be applied for Multiple-Input Multiple Output (MIMO) systems. Unlike SISO-NOMA, the channels of MIMO-NOMA are represented by matrices. Currently, there are two main designs for MIMO-NOMA 1) beamformer-based MIMO-NOMA and

2) cluster-based MIMO-NOMA. In the first design, different beams are directed towards different users and SIC is performed by users sharing the same resource block. Differently, cluster-based MIMO-NOMA divides users into several clusters, and each cluster is served by a single beam. Afterwards, SIC is used among users within the same cluster to recover the desired signals [14].

2.3 NOMA-based Applications

NOMA has become a key technology for 5G networks since it supports diverse requirements such as high data rates, increased spectral efficiency, and low latency. One major limitation is that users with low power levels/coefficients (near users) are able to recover the signals (information/data) of far users (high power levels) using SIC. Hence, enhancing the security of NOMA, especially in the downlink case, is essential to ensure the efficiency and robustness of systems employing this technology. The applications of NOMA are numerous (Fig. 3), and they include: heterogeneous networks [15], Machine-to-Machine (M2M) communication [16], Ultra-Dense Networks (UDN) [15], massive Machine Type Communications (mMTC) [17], Vehicle-to-Everything (V2X) [18], Device-to-Device (D2D) [18], Cooperative Relaying Networks (CRS) [19], massive MIMO [18], energy harvesting [20], millimeter wave communications [21], cognitive communications [22], physical layer security [23], Visible Light Communications (VLC) [24], Internet-of-Things (IoT) systems [23] and Mobile Edge Computing (MEC) [25].

3 Related Work

Physical Layer Security (PLS) has emerged as an optimistic technique to secure current and future communication systems in a lightweight and efficient manner. Particularly, users exploit the randomness of the shared channel between them to extract common parameters and achieve several security services such as device authentication, key generation, data confidentiality, source authentication and message integrity [18, 23]. Unlike conventional upper layer security solutions, PLS requires fewer rounds, and simpler operations per round, to achieve robust security while maintaining low overhead and minimum computational complexity. As a result, lately, PLS has attracted a lot of attention, and multiple PLS solutions have been presented targeting different communication systems and applications. Currently, most security schemes in the literature address the security of PD-NOMA, whereas few works focus on CD-NOMA [26]. This is attributed to the fact that CD-NOMA is similar to the legacy CDMA and thus, existing security solutions can be adapted for CD-NOMA [27]. Additionally, in CD-NOMA, each user has a unique non-orthogonal code, which can be designed in such a way that only the legitimate user and BS are aware of it [27]. On the other hand, from a PLS viewpoint, PD-NOMA has many challenges and limitations that should be highlighted and addressed. The security vulnerabilities of PD-NOMA are attributed to multiple factors [14]:

- The superimposed messages of multiple users are sent at the same time, over the same bandwidth. Hence, these information, which are sent in the clear (broadcast nature of wireless transmission), are vulnerable to being captured and leaked to illegitimate users.
- In order to recover the signal of each legitimate user, Successive Interference Cancellation (SIC) is applied. This process allows users to decode all of the transmitted signals (superim-

posed) to obtain the desired one. Hence, superimposed signals are not secure and are exposed to legitimate as well as illegitimate users.

In NOMA systems, adversaries could be either internal or external; an internal adversary is a NOMA user from the set of legitimate users in the network, whereas external adversaries do not belong to that set. The NOMA PLS schemes in the literature can be divided into eight classes as shown in Table 2:

1. Hashing the unique identifiers/parameters of users [28];
2. Relay [29, 30];
3. Cooperative jamming [31, 32];
4. Cognitive radio inspired NOMA [33];
5. Artificial noise [34, 35, 36];
6. Beamforming [37];
7. Optimization problems related to power/resource allocation and scheduling schemes [38]-[43];
8. Utilizing asymmetric cryptography for securing the signal of each user using public/private keys [44].

All of these schemes, except for asymmetric cryptography, enhance the security of the NOMA technology but not the security of the transmitted data itself. On the other hand, asymmetric cryptography is not practical for current and future systems since it requires multiple rounds and a large delay. Consequently, alternative solutions should be proposed and studied in order to improve the security of NOMA systems without degrading its performance.

4 Proposed Confidentiality Scheme

The proposed scheme consists of three steps: 1) key generation and cipher primitive derivation, 2) encryption/decryption scheme and 3) update process of the dynamic key and cipher primitives. We also discuss the possible cipher schemes that can be applied.

4.1 Dynamic Key Generation and Cipher Primitive Derivation Scheme

In any communication system, mutual authentication is first performed between the legitimate devices and the infrastructure (authentication server or base-station) and then, session keys are generated and exchanged to encrypt/decrypt transmitted data. Here, we assume that mutual authentication is achieved and that legitimate devices use their public/private keys to exchange important information such as the ID of the transmitter, the ID of the receiver, and the secret session key, SK.

The mutual authentication step and the connection establishment procedure will not be discussed further since they are not the main focus of this paper. It should be noted that any efficient key distribution protocol, such as those employed at upper layers, can be used to exchange SK

Table 2: A Summary of the PLS NOMA Schemes

Data confidentiality schemes	**Advantage**	**Limitation**	**Resource and communication overhead**	**Complexity**
Hashing unique identifiers/parameters of users	Authentication of users since only legitimate users will be able to generate the same hash digest	modifying the conventional SIC algorithm and increasing the delay for recovering the intended messages by using hash functions	During the SIC process, users need to perform two hashing operations	Computationally complex: hashing
Relay	Non-Repudiation between devices	Securing data requires two time slots (delay) and the relay is vulnerable to being impersonated	Confidentiality if achieved through multiple rounds of communication. Additional resources are required since in most cases the same data is sent several times	Not Computationally complex: decode and forward operation
Cooperative jamming	Complete data hiding from eavesdroppers	Synchronization between users is required. In addition, more resources, power and overhead are introduced	More power is needed to generate and send jamming signals	Computationally complex: jamming is an exhaustive operation
Cognitive radio inspired NOMA	Primary and secondary users are able to transmit data at the same time over the same time-frequency resources	Data is not protected from internal users	No additional cost and overhead	Not computationally complex
Artificial Noise (AN)	Automatic cancellation of AN when passing through the intended channel. No further actions done at the receiver	Eavesdropper can recover transmitted data if it is aligned with the legitimate receiver. Transmitted data is not encrypted	Generation of AN	1) Channel estimation. 2) generation of AN. 3) Appending AN to the transmitted data
Beamforming	Simple and it does not require any additional overhead	If illegitimate users are aligned with the legitimate users they will be able to recover the transmitted signals. The information of internal users is not secured from each other	It does not require additional resources or communication overhead	not computationally complex
Optimization problem of power/resource allocation and scheduling schemes	Theoretical analysis and mathematical derivations	These scheme do not secure transmitted data itself	Additional resources and communicated messages are required for scheduling algorithms between the BS and the legitimate user	Most optimization problems presented in the literature are non-convex, hence, they are very complex algorithms
Securing transmitted data using asymmetric encryption	No one except the legitimate user can decode its signals due to the confidentiality of the private key	asymmetric encryption is unpractical requires additional resources and overhead	1) secure exchange of public keys. 2) encryption using public keys. 3) decryption using private keys	asymmetric encryption requires multiple rounds (high complexity)

between each device and the base station. Next, all of the K legitimate devices in a specific cell, D_i ($i = 1,\ 2,\ \ldots,\ K$), and the base-station (or gateway) perform channel estimation and reconciliation to obtain the i^{th} Channel Impulse Response (CIR) of each user:

$$Ch_i = [Ch_{i,1}, Ch_{i,2}, \ldots Ch_{i,l}]^T, \tag{4}$$

where $Ch_{i,l}$ is the channel gain belonging to the largest path delay, l is the length of Ch_i and $(\cdot)^T$ is the transpose operation.

Using the above parameters, a dynamic encryption key, DK_i, is derived by the legitimate device, D_i, and base station (gateway), as follows:

$$DK_i = H(Ch_i) \oplus SK_i, \quad i = 1, 2, \ldots, K \tag{5}$$

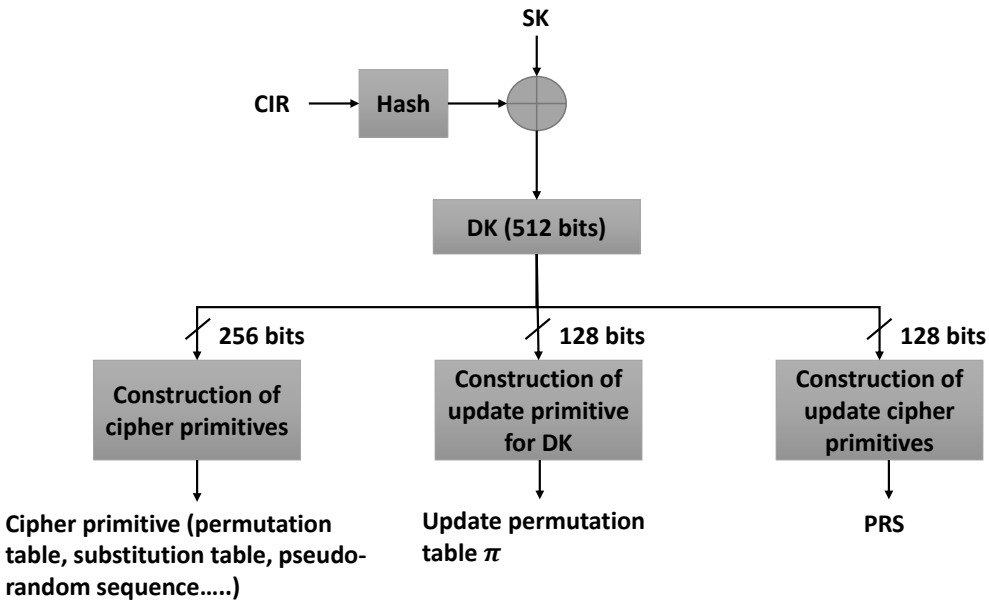


Figure 4: Proposed key distribution scheme

where $\oplus$ represents the XOR operation, and $H(\cdot)$ corresponds to the secure hash function $SHA-512$. First, the i^{th} Channel Impulse Response, Ch_i, is hashed, then XORed with the session key, SK_i, to produce the dynamic key DK_i (512 bits). If the two XORed values do not have the same length, padding is applied. Here, Ch_i introduces dynamicity and randomness (physical layer), and is considered as a second factor for achieving data confidentiality in the proposed scheme. This step is repeated K times, so that all NOMA users in a specific cell are able to generate unique dynamic keys, which are needed to protect transmitted data from internal, as well as external users.

Next, three sub-keys, of lengths 256, 128 and 128 bits, are produced from the dynamic key, as illustrated in Fig. 4. The first sub-key is used to generate the cipher primitives needed to encrypt the data of each NOMA user (depends on the selected operation such as permutation, substitution, masking, and phase scrambling). The second sub-key is used to generate an update permutation table, π, which is used to update (pseudo-randomly permute or shuffle) the dynamic key for every

new input frame (frame consists of a set symbols). π has the same length of the dynamic key. Finally, the third sub-key is used to derive PRS which is a pseudo-random sequence, having a size equal to one frame. More specifically, the number of elements in PRS is equal to number of frame symbols in one frame ($1 \times N$). For every new input frame symbol, the PRS is used to circularly shift the utilized cipher primitives (updating process according to the corresponding PRS value).

For the construction of cipher primitives (permutation or substitution tables), the techniques presented in [45] are adopted. For the masking and phase shuffling cipher primitives, key-stream sequences are required; these can be generated using any stream cipher.

4.2 Encryption Scheme

In a typical digital communication system, input data is encoded using source and channel encoding, and then modulated. Here, any M-QAM (Quadrature Amplitude Modulation) scheme can be used such as 4-QAM, 16-QAM, 64-QAM or 256-QAM. The main difference between these schemes is the number of bits, m, that gets mapped to one constellation point (modulation symbol). Consequently, each modulation scheme has $M = 2^m$ complex modulation symbols. Following modulation, the proposed dynamic key-dependent cipher scheme is applied to each modulation symbol, to obtain the encrypted frame symbol, and consequently the overall frame, which contains N frame symbols. The proposed scheme is generic in the sense that any simple and efficient encryption operation, such as substitution, permutation, phase encryption or masking, can be applied in this step. Several possible encryption schemes that can be applied in the proposed solution are discussed in detail, in the following subsection.

The contents of each frame symbol (containing multiple modulation symbols) are encrypted using the previously derived cipher primitives, and which correspond to a specific cipher scheme (for example, the permutation scheme). Hence, the superimposed downlink signal becomes:

$$x(t) = \sum_{i=1}^{K} \sqrt{\alpha_i P_{BS}} c_i(t), \tag{6}$$

where, $c_i(t)$ is the encrypted signal of user i.

As such, the superimposed signals of PD-NOMA users are secured against internal and external users, since each user is only able to recover his signal using the corresponding physical channel parameters and a shared secret. This is important since NOMA allows users with stronger signals (near the base station) to decode and recover the signals of weaker users (far from the base station).

The proposed scheme can also be applied in the uplink case (against external users only), since NOMA users and the base station are able to extract the same channel-based parameters and they share a common secret, hence the base station will be able to successfully decode the signals of each user. However, the security of data in downlink NOMA is more critical and crucial (vulnerability against external and internal users). The proposed uplink signal becomes:

$$y(t) = \sum_{i=1}^{K} Ch_i c_i(t) + n_i(t). \tag{7}$$

At the receiver's side, the same steps are required for decryption but in a reversed order and using the inverse cipher primitives.

4.3 Possible Encryption Schemes

As indicated previously, all presented cipher schemes of [7] can be used in the proposed solution. In this part, two main PLS encryption algorithms and their variants are presented and discussed.

4.3.1 Phase-amplitude encryption

The phase-amplitude encryption scheme of [7] (described in Algorithm 1) requires three binary pseudo-random sequences a b, and c. These sequences can be generated using a stream cipher that inputs a secret key as a seed. In contrast to c, sequences a and b are transformed from binary representation $\{0, 1\}$ to polar $\{-1, 1\}$ as follows:

$$a \leftarrow 2 \times a - 1 \quad \text{and} \quad b \leftarrow 2 \times b - 1. \tag{8}$$

Afterwards, each value of a and b is multiplied by the real and imaginary parts of a modulation symbol, respectively. The third sequence c was introduced in [16], where the real and imaginary parts of each modulation symbol are shuffled when the corresponding value of c is equal to '1' (Algorithm 1). The decryption algorithm is similar to the encryption process but in a reversed order. This indicates that both the encryption and decryption procedures require the same amount of resources and latency.

Algorithm 1 Phase-amplitude encryption scheme

```
1:  procedure PHASE_AMPLITUDE_ENCRYPTION
        (Frame symbol FS, a, b, c)
2:      for i = 1 to length(FS) do
4:          x[i] = Real(FS[i])
5:          y[i] = Imaginary(FS[i])
6:          if c[i] == 1 then
7:              temp = x[i]
8:              x[i] = y[i]
9:              y[i] = temp
10:         EFS[i] = a[i] × x[i] + j × b[i] × y[i]
11:     return EFS
```

In order to adopt the phase-amplitude encryption scheme in the proposed solution, three sequences (a, b and c) each having a size equal to the size of one frame symbol, are generated. The frame symbol contains a number of complex modulation symbols. Next, one element from each sequence is used to encryption one complex symbol in the frame symbol. When the chosen element from sequence c is equal to '1', the real and imaginary components of the complex symbol are first shuffled, and then multiplied by the elements chosen from sequences a and b. Otherwise, the real and imaginary components of the complex symbol are directly multiplied without permuting them. In this way, the phase (having either a '+' or '-' sign) and the amplitude of each complex symbol are randomly encrypted. For every new frame symbol (containing a new set of complex modulation symbols) and for every new frame, the used sequences are updated in an efficient manner.

Note that the phase-amplitude encryption scheme is a variant of the phase encryption scheme, which utilizes only two binary key-streams (a and b). The difference between both schemes is

Algorithm 2 Permutation Encryption Algorithm.

Input: j^{th} Data Frame Symbol FS_j, Permutation table π, and length of frame symbol α
Output: j^{th} Encrypted Data frame Symbol FS_j

1: **procedure** PERMUTATION_ENCRYPTION(FS_j, π, α)
2: **for** $ind = 1$ to α **do**
3: $temp2 = FS_j[ind]$
4: $FFS_j[ind] = FS_j[\pi[ind]]$
5: $FFS_j[\pi[ind]] = temp2$
6: **return** EFS_j

that the phase encryption scheme doesn't shuffle the real and imaginary parts of each modulation symbol.

4.3.2 Permutation cipher scheme

The permutation scheme can be either realized by 1) using a permutation table or 2) applying a random cyclic delay (perturbation) to transmitted signals. Permutation has several advantages such as: simplicity, low computational complexity and low resources.

Compared to the previous scheme, the permutation scheme does not divide the symbols into real and imaginary. It is performed at the modulation symbol level (complex value) and it only depends on symbol shuffling (1-D permutation) (Algorithm 2). Hence, this scheme requires fewer operations compared to the phase-amplitude encryption scheme. The decryption algorithm is similar to encryption, however, it requires an inverse permutation table instead of the original permutation table.

Again, in order to adopt the permutation operation in the proposed solution, a permutation table having a size (dimensions) equal to that of one frame symbol, is generated. Here, the contents of each frame symbol are permuted/shuffled (the locations of complex modulations are randomly changed). For every new frame symbol and for every new frame, the permutation table is updated, so that each frame symbol is encrypted using a different (modified) permutation table.

These ciphers are employed in the proposed solution and the corresponding performance and security results are presented in the subsequent sections.

4.4 Update Process of the Dynamic Key and Cipher Primitives

For every new frame, the dynamic key is updated using the permutation table π, which is a simple and low cost technique. Circular shifting depends on the produced PRS having a length equal to N. If the j^{th} PRS value is equal to r, then the cipher primitive of the j^{th} frame symbol is shifted r times. For the permutation cipher primitive, this is realized by shifting the values of the permutation table r locations. As for the phase-amplitude scheme, the update process is realized by shifting each of the three sequences, a, b and c, r times based on the PRS.

Figure 5 represents the proposed structure of the update cipher primitive process, which relies on the channel-based dynamic key to create and update the needed cryptographic primitives. The encrypted data frame symbol (EFS) is derived by simply applying the proposed one-round, one-operation cipher scheme. The generated cipher primitive(s) are updated, frequently. Specifically,

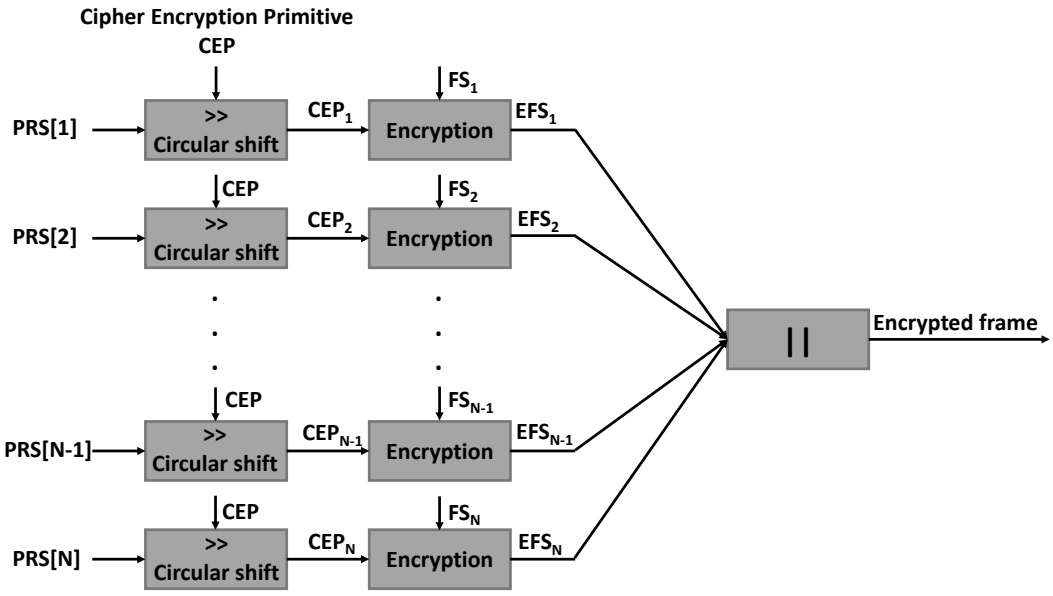


Figure 5: The proposed update process of the cipher primitives

they are circularly shifted after each new frame symbol (FS), depending on the value of PRS. The error propagation effect is reduced since the encryption scheme is applied at the modulation symbol level, which prevents an erroneous symbol from affecting other modulation symbols.

The main advantage of the proposed update cipher primitive scheme is enabling parallel computing and parallel ciphering, which reduces the required latency and delay. In fact, one can pre-compute all of the updated cipher primitives and the dynamic keys ahead of time, according to the generated PRS and π.

Moreover, the update cipher primitive operation increases the robustness and security level of the solution against different types of attacks.

The detailed flowchart of the proposed scheme is shown in Fig. 6. It includes all of the discussed steps, and which are summarized below:

1. **Step 1:** The legitimate devices and the base station perform channel estimation and reconciliation to obtain the channel impulse response of each device in the cell (gather channel information and characteristics which are unique to each device). Moreover, each device shares a unique secret key with the base station (pre-shared key).

2. **Step 2:** To obtain the dynamic keys, devices and the base station combine (XOR) the secret key with the hashed channel parameters (dynamic).

3. **Step 3:** Then, the dynamic key is divided into three sub-keys.

    - The first sub-key is used to generate the required cipher primitives that are used during the encryption/decryption process of data (frame symbols). An example of possible employed cipher primitives is a dynamic permutation table.

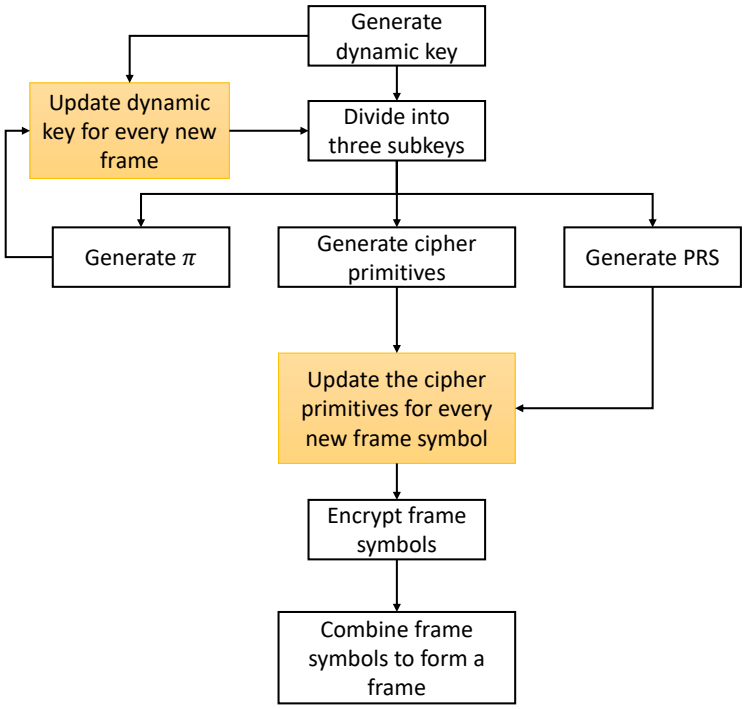


Figure 6: The flowchart of the proposed scheme

- The second sub-key is used to generate the required update permutation table (update dynamic key primitives) that is used to permute (update) the dynamic key for each new frame.
- The last sub-key is used to generate the update cipher primitives (PRS). This update cipher primitive is employed to shuffle cipher primitives after each new frame symbol. Consequently, this update process hinders existing cryptanalysis mechanisms and safeguards against a large number of attacks.

4. **Step 4:** The data (consisting of frame symbols) of various devices is encrypted (each using different cipher primitives) and then superimposed using different power levels. The overall signal is then transmitted to the base station. The proposed technique can be applied in the uplink and downlink cases. Here, any cipher primitive can be used such as permutation or phase encryption.

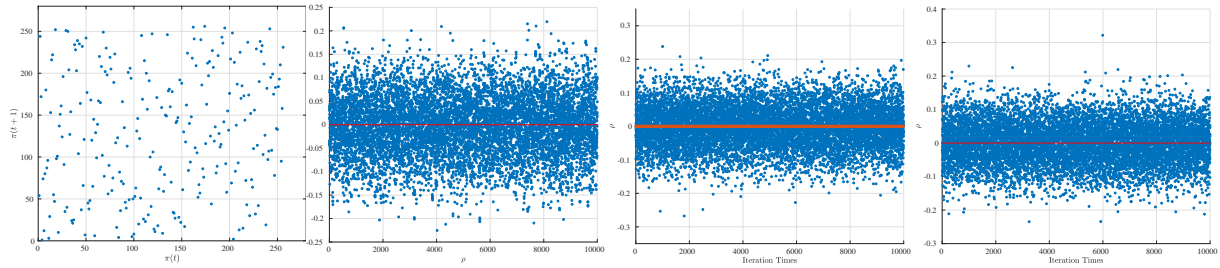
5. **Step 5:** For every new frame symbol, the cipher primitives are updated (circular shifting) using the PRS. On the other hand, the dynamic key is updated/changed using π for every new frame (permuted). For the encryption of new frame symbols, the same steps that are mentioned above are carried out.

For the decryption algorithm, it is only required to compute the inverse cipher primitives for each frame symbol.

5 Security Analysis

In this section, we assess and analyze the security level of the cipher scheme. We conduct tests related to randomness, uniformity, independence and sensitivity to evaluate the generated cryptographic primitives. The update cipher primitive technique is also evaluated against the desired security properties. It should be noted that the employed metrics are well-known and sufficient to quantify the security level at the physical layer [7, 18].

In this study, we have used three popular cipher schemes which are: permutation, phase encryption and phase-amplitude encryption [23].



(a) (b) (c) (d)

Figure 7: (a) The recurrence of a randomly-generated permutation table, (b) the correlation coefficient of the recurrence of 1,000 randomly-generated permutation tables, (c) the correlation coefficient between a randomly-generated permutation table and its updated version, and (d) the coefficient correlation between two subsequent permutation tables

5.1 Evaluation of the Proposed Update Process

In this sub-section, the performance of the proposed "update cipher primitive technique" is studied and quantified in order to prove its secure deployment in different cipher schemes. We consider the cipher primitive of the permutation scheme and we apply the proposed update technique on the produced permutation boxes (tables). It should be noted that the cipher primitives of any cipher scheme can be considered and tested. Therefore, a simulation study that tests the recurrence and correlation (ρ) of updated permutation tables is applied using $1,000$ random dynamic keys and for different input frames.

The recurrence of a randomly produced permutation box is shown in Fig. 7a. This plot is widely scattered and randomly distributed, which demonstrates the desired outcome (high randomness degree). Figure 7b, on the other hand, shows the correlation between multiple recurrence plots corresponding to different permutation tables produced by employing $1,000$ random dynamic keys. The produced permutation tables exhibit a high degree of randomness for any dynamic key since the correlation coefficient of the recurrence values is always close to the ideal value, 0.

The correlation between the original permutation table and its updated one can be seen in Figure 7c; the value is always close to zero, confirming that the original permutation table is independent from the updated one. Another correlation test is also shown in Fig. 7d. This test is conducted between two successive (updated) permutation tables for $1,000$ iterations; the results reveal the independence of any two successive permutation tables.

The obtained results prove that the proposed update technique is highly secure and efficient since no correlation exists in all of the considered cases. This results in a high robustness degree against passive attacks, and prevents any information leakage to adversaries.

Table 3: Statistical results for 1000 update permutation iterations

Coefficient Correlation Tests	Min	Mean	Max	Std
ρ of the recurrence of produced dynamic permutation tables	-0.20408	-0.00372	0.22361	0.06297
ρ between the primary permutation table and its updated version (permuted version)	-0.23755	0.00002	0.27322	0.06255
ρ between two successive permutation tables	-0.24947	0.00028	0.23183	0.06264

In Table 3, statistical analysis also confirms the high level of independence between updated permutation tables. According to the presented results, the standard deviation of the listed cases is very close to 0, which implies that the correlation values are near the desired mean value.

The obtained results indicate that the primary permutation table and the updated ones are highly uncorrelated. Also, these results validate the independence between any two successive update permutation tables. Consequently, the update permutation tables attain a high randomness and uniqueness degree which prevents unauthorized users from extracting any useful information and prevents eavesdropping. Consequently, the proposed solution is immune against current techniques of cryptanalysis.

5.2 Statistical Analysis of Encrypted Symbols

In principle, the produced ciphertext of a secure cipher scheme should resist statistical attacks, which requires achieving high levels of randomness and uniformity. Therefore, in the following, the randomness, uniformity and independence properties of the obtained encrypted frames are analyzed to confirm the immunity of the proposed cipher against different types of statistical attacks.

5.2.1 Uniformity Property

In order to evaluate the uniformity property, the Empirical Cumulative Distribution Function (ECDF) is used to assess the generated ciphertext, visually.

The ECDF of the plaintext and ciphertext frames are illustrated in Figures 9c and 9f, when using the dynamic permutation operation as an encryption scheme, at the modulation symbol level. The obtained ciphertext clearly satisfies the required uniformity level. Similar results are obtained for phase encryption ('AB' cipher scheme) and phase-amplitude encryption ('ABC' cipher scheme). Uniformity can also be statistically evaluated using the entropy test (based on the probability values):

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log_b P(x_i). \tag{9}$$

The entropy results in Figure 8 show that for all tested cipher schemes (permutation, AB and ABC), the desired entropy value is attained. The ideal entropy value at the byte level is 8, and which represents maximum uncertainty (revealing new and unknown information). In contrast, the

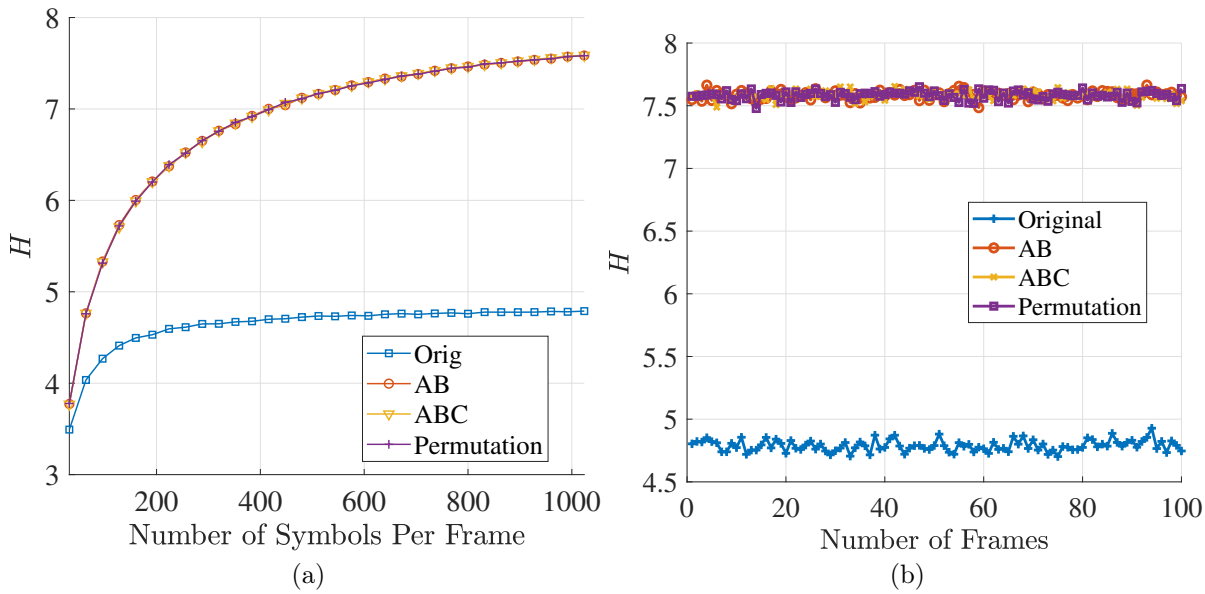


Figure 8: Results of the entropy test of the plaintext and ciphertext using three different cipher techniques versus (a) the number of symbols per frame and (b) the number of frame

original data has entropy values less than 8 (varying around 4.7) since it is normally distributed, hence, it has a lower uncertainty degree (Table 4).

Table 4: Entropy values corresponding to the statistical analysis the original and encrypted frame symbols

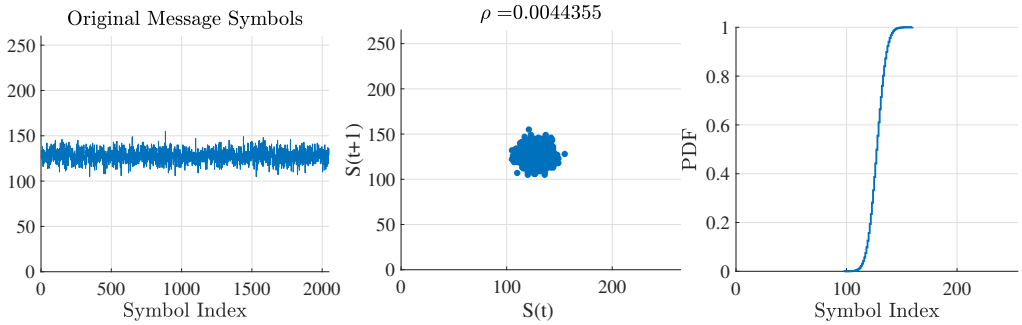
Entropy Test	Min	Mean	Max	Std
Original frames	4.702	4.789	4.928	0.045
Ciphertext with AB cipher scheme	7.485	7.584	7.665	0.033
Ciphertext with ABC cipher scheme	7.489	7.586	7.654	0.034
Ciphertext with Permutation cipher scheme	7.478	7.583	7.652	0.033

5.2.2 Randomness Property

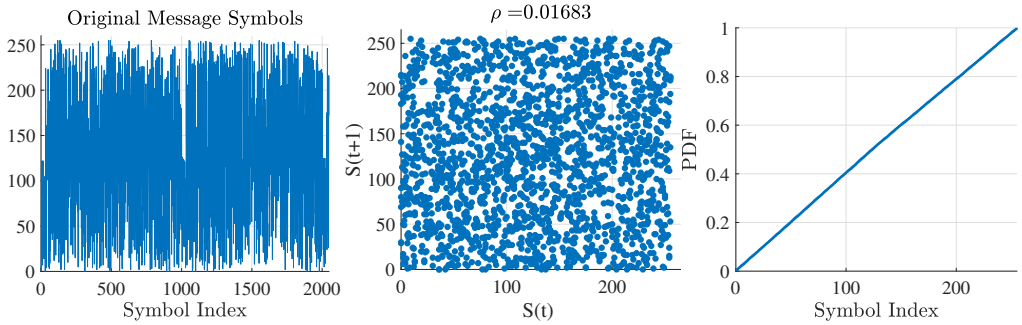
The recurrence test can be used to measure the randomness level of encrypted symbols within the message space; the encrypted frames should have a uniform distribution. On the other hand, the correlation coefficient of the recurrence test should be equal or close to zero, which confirms the internal independence among encrypted frames. These tests are necessary to quantify the randomness and independence properties.

Figure 9b shows that the original data recurrence plot has a normal distribution (very low randomness degree). Whereas, Fig. 9e shows the recurrence plot of the obtained encrypted message (permuted modulation symbols). Results show that encrypted symbols are randomly scattered and distributed, which ensures a good randomness level. Moreover, as seen in Fig. 9a, the original frame symbol has a fixed amplitude range, while Fig. 9d shows that the encrypted symbols have

random varying amplitudes. Finally, similar results were obtained for both, the phase encryption and phase-amplitude encryption schemes.



(a) Symbol amplitude of original data (b) Recurrence of original data (c) ECDF of original data



(d) Symbol amplitude of permuted data (e) Recurrence of permuted data (f) ECDF of permuted data

Figure 9: Symbol amplitude of (a) original and (d) permuted data. Recurrence of (b) original and (e) permuted data. ECDF of (c) original and (f) permuted data

Next, we have performed the cross-correlation test of the recurrence of ciphered frames (Figures 10a and 10b). The desired value of the recurrence cross-correlation should be close to 0, to confirm that encrypted frames reach a high level of randomness.

The recurrence correlation coefficients is close to the desired value, 0, for all encryption schemes (permutation, phase encryption and phase-amplitude encryption schemes). Table 5 complements the results in Figures 10a and 10b.

Table 5: Test values corresponding to the statistical analysis of the correlation coefficient of the recurrence of ciphertext

ρ of the recurrence of ciphertext	Min	Mean	Max	Std
AB cipher scheme	-0.062	0.041	0.127	0.038
ABC cipher scheme	-0.067	0.044	0.166	0.046
Permutation cipher scheme	-0.1	0.031	0.158	0.047

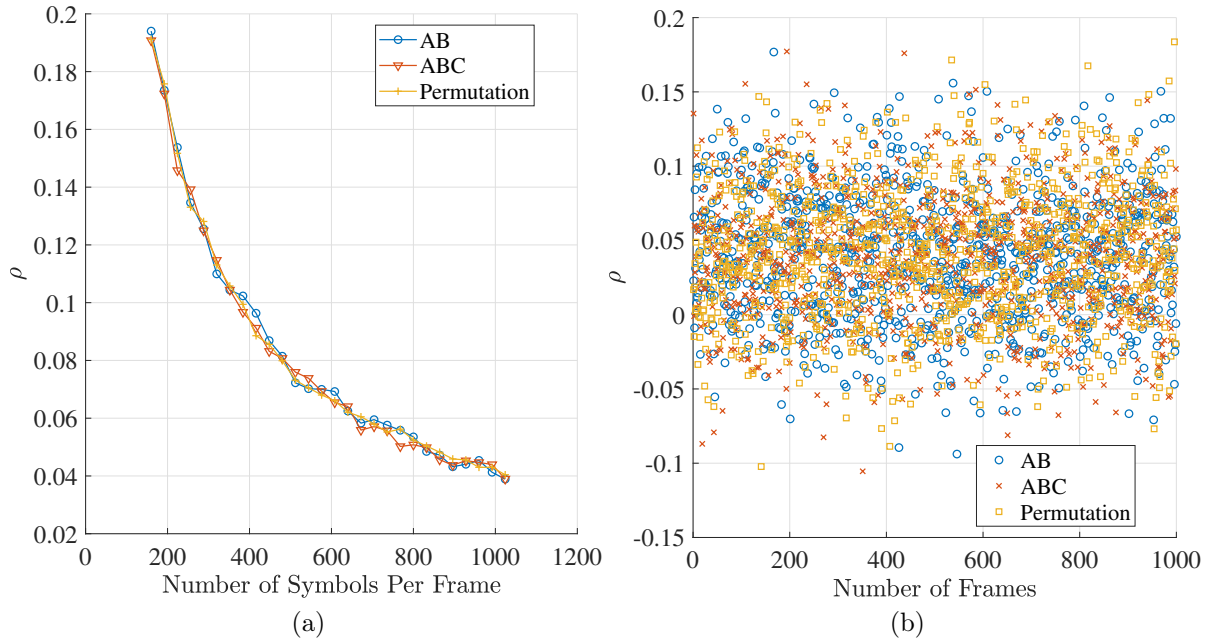


Figure 10: Results of the correlation coefficient of the recurrence of ciphertext using three different cipher techniques versus (a) the number of symbols per frame and (b) the number of frame

5.2.3 Independence

To achieve independence, the difference between the original and encrypted symbols should be equal to 50% at the bit level. This property is crucial for ensuring the proposed scheme's immunity against statistical attacks. Difference is computed using the following equation:

$$DIF = \frac{\sum_{i=1}^{N} dec2bin(FS_i) \oplus dec2bin(E_{DK}(FS_i))}{T}, \tag{10}$$

where N is the number of frame symbols in one frame, and T is the length of one frame symbol.

Figures 11a and 11b correspond to the average difference between the original and encrypted frames when varying the number of bits per symbol and the number of symbols per frame, for 1,000 iterations, respectively. Figure 11c represents the Effective Cumulative Density Function for 1,000 frames symbols. As it can be depicted in Fig. 11, all encryption schemes have a difference value close to the desired value (0.5) for 1,000 transmitted frames. This is also confirmed in Table 6.

Table 6: Test values corresponding to the statistical analysis of the difference values

Difference Test	Min	Mean	Max	Std
AB cipher scheme	0.472	0.5	0.517	0.008
ABC cipher scheme	0.473	0.5	0.517	0.008
Permutation cipher scheme	0.477	0.499	0.516	0.008

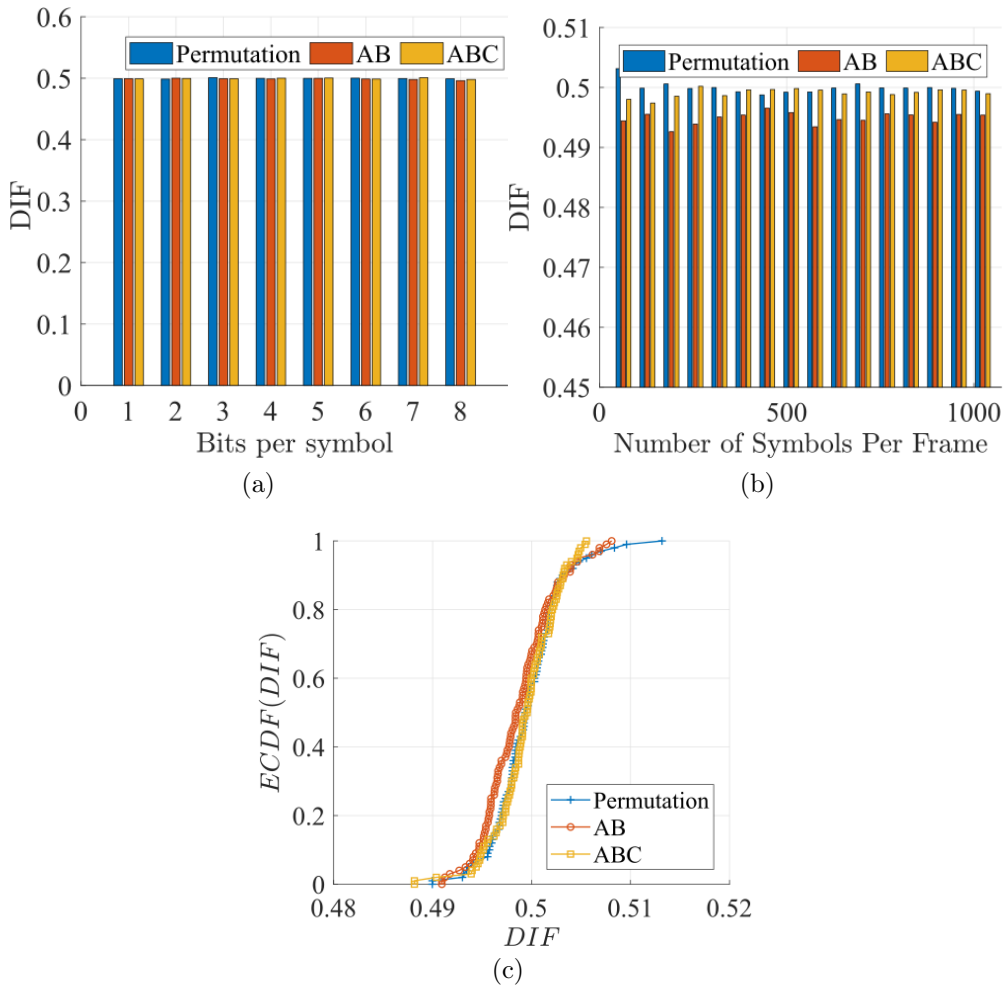


Figure 11: Independence test to measure the difference between plaintext and ciphertext using three different cipher schemes, versus (a) the number of bits per modulation symbol, (b) the number of modulation symbols per frame symbol, and (c) the corresponding effective cumulative density function for 1000 frame symbols

The second test is based on the cross-correlation between plaintext and ciphered frames. The desired value of the cross-correlation should be close to 0, to confirm the independence of the original and encrypted frames.

The correlation coefficients between the plaintext and ciphered frames is close to the desired value, 0, for all encryption schemes (permutation, phase encryption ('AB' scheme) and phase-amplitude encryption schemes ('ABC' scheme)) based on three cases: 1) bits per symbol (Fig. 12a), 2) symbols per frame (Fig. 12b), 3) and number of transmitted frames (Fig. 12c). Table 7 also validates the above results.

The obtained results prove that the proposed cipher scheme fulfills the desired security metrics, which makes it immune against statistical attacks.

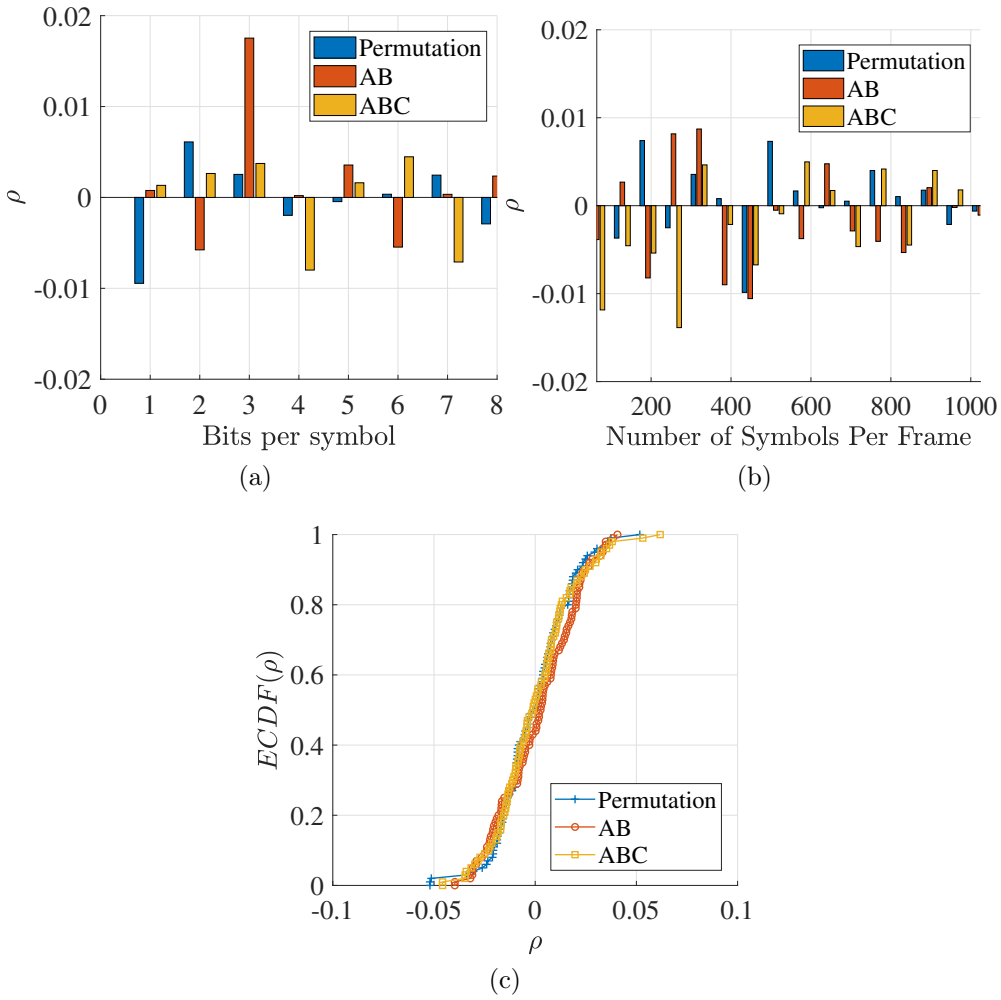


Figure 12: Results of the correlation coefficients between the plaintext and ciphertext using three different cipher techniques versus three cases: (a) the number of bits per modulation symbol, (b) the number of modulation symbols per frame, and (c) the number of frame symbols transmitted

Table 7: Test values corresponding to the statistical analysis of correlation test between the original and encrypted frames symbols

ρ between plaintext and ciphertext	Min	Mean	Max	Std
AB cipher scheme	-0.11	0.004	0.098	0.0430
ABC cipher scheme	-0.099	0.004	0.115	0.0430
Permutation cipher scheme	-0.113	-0.003	0.098	0.0440

5.3 Sensitivity Analysis

Sensitivity tests are used to analyze the key and plaintext sensitivities to prove that the avalanche effect is reached, in both cases. These tests are performed in order to quantify the difference

probability between two encrypted frames symbols when one bit differs in the original frame and in the secret dynamic key. The desired value is 0.5 probability, at the bit level.

5.3.1 Key Sensitivity

The key sensitivity test measures the bit difference between two encrypted frames when using two keys, DK and DK', which differ by only one bit. The difference, at the bit level, should be always close to 50%, and it is calculated as follows:

$$KS = \frac{\sum_{i=1}^{N} dec2bin(E_{DK}(FS_i)) \oplus dec2bin(E_{DK'}(FS_i))}{T}, \tag{11}$$

where T is the bit length of the original and encrypted frame symbols.

This test was applied to all encryption schemes, where two secret dynamic keys (DK and DK') are used for each iteration to encrypt the same original data frame. Then, the hamming distance is calculated at the bit level.

Figure 13 and Table 8 show the results of key sensitivity for 1,000 iterations. All of the key sensitivity values and for all simulation cases, are very close to the desired value that is 0.5 (the number bits per symbol (Fig. 13a), the number of symbols per frame (Fig. 13b) or the number of transmitted frames (Fig. 13c)).

Table 8: Test values corresponding to the statistical analysis of key sensitivity

Key Sensitivity Test	Min	Mean	Max	Std
AB cipher scheme	0.477	0.5	0.52	0.008
ABC cipher scheme	0.486	0.502	0.517	0.007
Permutation cipher scheme	0.482	0.499	0.521	0.007

5.3.2 Plain-text Sensitivity

In this work, we exclude the plain-text sensitivity since different cryptographic primitives are used for different frames, which results into completely different ciphertexts. As such, the scheme inherently satisfies the plain-text avalanche effect based on the key avalanche effect.

6 Cryptanalysis

The security level of the proposed scheme is directly related to its ability to resist existing cryptanalysis attacks such as ciphertext-only, chosen/known plaintext/ciphertext and brute force attacks. The proposed scheme requires a one iteration round and a single operation. It benefits from the concept of “dynamic cryptography" (cryptographic primitives that change frequently and dynamically) to prevent the disclosure of useful information from encrypted frames. In the following, we prove that the proposed cipher approach is immune against the previously listed attacks.

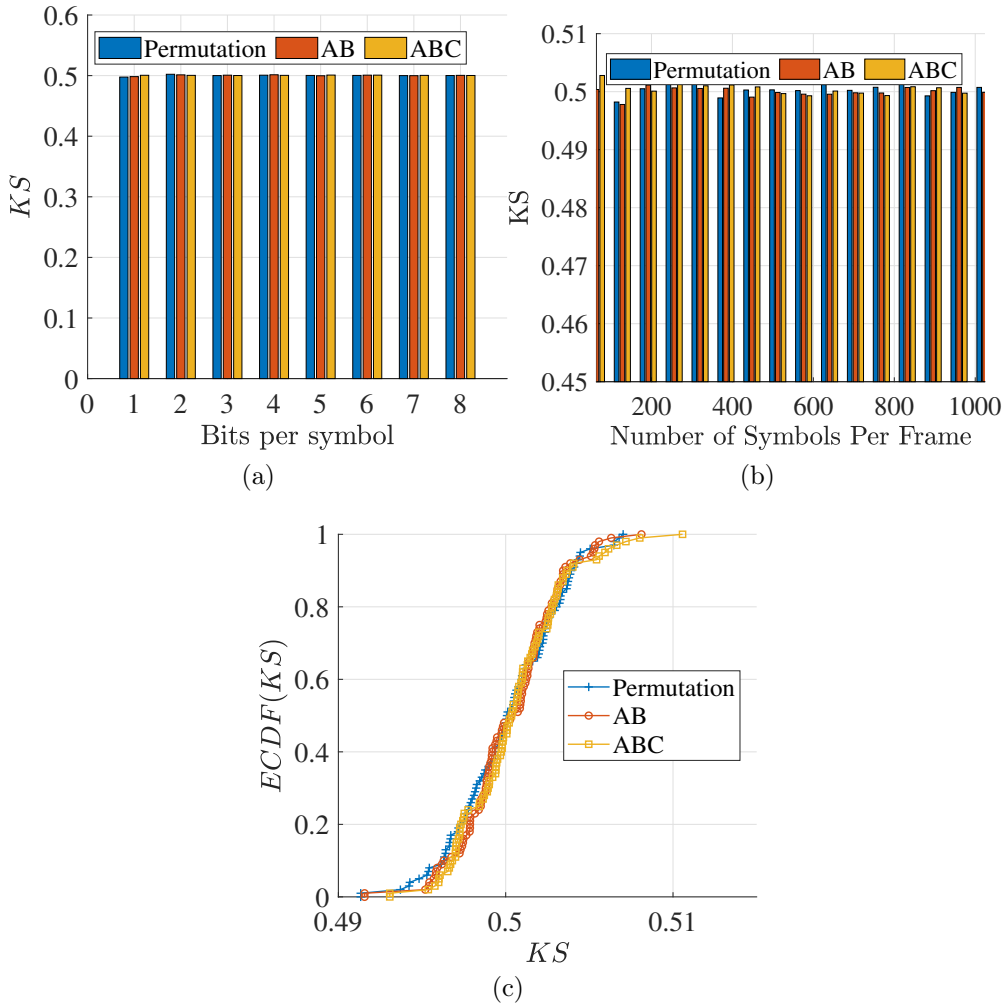


Figure 13: Results of key sensitivity versus (a) number of bits per symbol, (b) number of modulation symbols per frame, and (c) number of frames symbols transmitted

6.1 Resistance Against Ciphertext-Only (Statistical) Attacks

To guard against statistical attacks, the proposed cipher scheme should produce ciphertext that has a high level of randomness and a uniform distribution. These properties have been proven using the results presented in Section 5.

In general, the security degree of the proposed scheme is influenced by the randomness and uniformity of the generated dynamic keys and ciphertext. As shown in the previous section, the desired randomness and uniformity levels of the ciphertext and dynamic keys are reached, whereby the ECDF is close to a uniform distribution. Moreover, the obtained results in Fig. 9e show that the encrypted symbols are highly scattered (randomized/non-linear). Two other tests have also been applied, and which are the coefficient correlation test and difference test (the percentage difference) between the original frame symbol and its corresponding encrypted version for $1,000$ iterations. Figures 11 and 12 clearly prove that unencrypted and encrypted frame symbols are completely

independent of each other. The independence property is validated since the difference probability is always close to 0.5 and the correlation coefficient between original and encrypted frames is always close to 0.

Furthermore, Tables 5, 6 and 7 show the statistical results of 1) the correlation test of the recurrence, 2) the correlation coefficient between plaintext and ciphertext, and 3) the probability difference between plaintext and ciphertext. The mean values of the first two correlation tests are close to the ideal value, which is 0. In contrast, the mean value of the probability difference is equal to the desired which is 0.5. The standard deviation in all tests is very small, meaning that the results are always close to the mean value. Additionally, a low standard deviation value leads to a small variation between the minimum and the maximum values. For all tests, the generated outcomes are close to the ideal values. Thus, the presented statistical tests confirm the robustness of the proposed approach, and its high resistance against statistical attacks.

6.2 Resistance Against Chosen/Know Plaintext/Ciphertext Attacks

The key sensitivity test has proven that a completely different ciphertext is obtained (50% variation at the bit level) when a single bit of the secret key is changed. In the proposed approach, key sensitivity is ensured since all of the cipher primitives and update cipher primitives depend on the produced dynamic key and they change constantly.

The key sensitivity test is applied for $1,000$ iterations. In fact, the slightest change in the nonce or secret key will lead to a different dynamic key and, consequently, a different set of cipher and update cipher primitives (a difference probability of at least 0.5). This is illustrated in Fig. 13 which proves that two encrypted messages, obtained using two slightly different keys, DK and DK', are totally different and independent. Therefore, the proposed cipher solution is robust against linear/differential attacks.

Table 8 validates the key sensitivity property where the average is always close to the ideal value and the standard deviation value is very low. This indicates that most key sensitivity values vary around 0.5. As a result, unauthorized users can not obtain valuable information and the proposed scheme is immune against chosen/known plaintext/ciphertext attacks.

6.3 Related Key Attacks

Unlike conventional static cipher schemes, the proposed scheme relies on a dynamic cryptographic structure. Moreover, results from Figure 13 show that the desired key sensitivity (0.5) probability is successfully reached. Therefore, the proposed scheme can resist related key attacks.

Furthermore, the issues related to single frame failure and accidental key disclosure are avoided using the dynamic key scheme. Any change in any bit of the secret key or channel causes a significant change in the dynamic key, the produced cryptographic primitives, the update cryptographic primitives, and the encrypted frames.

6.4 Resistance Against Brute-force Attacks

The dynamic key has a 512-bit length, while the length of the secret session key can be 128, 196, or 256 bits. The nonce has a length of 512 bits since it is obtained by hashing the Channel Impulse Response (CIR) using the SHA-512 algorithm. Let us indicate that the proposed scheme minimizes

the Key Disagreement Rate (KDR) between users since information reconciliation is applied after channel estimation. In this step, users make sure that the CIR generated at both ends is the same.

As a result, the brute force attack is thwarted by the proposed scheme as the dynamic key space is 2^{512}, the nonce space is 2^{512}, and the session secret key is (at least) 2^{128}. All are considered large enough to hinder brute-force attacks. It is important to note that the secret session key is padded with zeros such that it has the same length as the channel nonce. This is crucial for executing the XOR operation.

6.5 Resistance Against Weak Keys

The dynamic key is obtained using the proposed dynamic key derivation scheme and it is divided into a set of dynamic sub-keys. These sub-keys have different functionalities: the first sub-key is used to produce the required cipher primitives, the second is used to produce the update permutation table for the dynamic key and the third sub-key is used to update the cipher primitives. Cipher primitives depend on the chosen cipher scheme, where it is a permutation table in the case of the permutation cipher scheme. As previously stated, cipher primitive(s) can be updated for each new input frame symbol. By updating the cipher primitives regularly, independent ciphertexts are derived and which in turn guards against any dynamic key disclosure accidents. This makes the attacker's task more challenging. The maximum cryptographic strength is, thus, achieved. It should also be noted that the main benefit of this proposed scheme is that any vulnerability in any frame symbol (sub-frame) would not affect any other data frame symbols.

6.6 Robustness Against Future Attacks

Finally, the use of dynamic cipher primitives, which change for every input frame and each frame symbol, increases the immunity of the proposed cipher scheme against typical or future attacks.

In this section, a cryptanalysis discussion has been presented to validate the security of the proposed scheme, its robustness and its applicability in current and future NOMA power domain systems. The proposed cipher solution can successfully resist current and future attacks such as ciphertext only and brute force attacks. The main argument that demonstrates the robustness of the proposed solution is that all existing cryptanalysis techniques are built around the concept of a static secret key and static cipher primitives (same cipher primitives are used for all parts of the message). This, in turn, prevents current cryptanalysis techniques from compromising the proposed dynamic scheme. New cryptanalysis techniques might be necessary to break "dynamic cipher schemes". Currently, there are no schemes of this sort, yet.

7 Performance Evaluation

In this section, we adopt several performance criteria and we perform several tests to prove the efficiency of the proposed cipher scheme, and its ability to adapt to several practical cases in wireless NOMA communication systems. In fact, for a cipher scheme to be considered efficient, it must require low memory consumption, low latency, and minimal resources. Theoretically, this can be proven since the proposed PLS cipher scheme uses a single round structure with simple operations.

Throughout this section, the computational complexity, latency and error propagation are quantified. In addition the required execution time for each encryption scheme is computed and measured, in addition to the effect of error propagation.

7.1 Computational Complexity

The computational delay of the proposed one round one-operation cipher scheme is evaluated in this part of the paper. The proposed cipher scheme aims at reaching robust security with minimal overhead (number of operations and round iterations). To assess 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 requires the highest delay compared to the 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. En_t denotes the time required by the chosen encryption operation, such as permutation.
8. U_t represents the time required by the update operation, which is permutation.
9. π_t is the time needed by the permutation operation.

First, we calculate the total computation delay that is required by the traditional AES (Advanced Encryption Standard) scheme [46]:

$$CD_{AES} = r_o Sb_t + (r_o + 1)xor_t + (r_o - 1)MC_t + r_o SR_t, \tag{12}$$

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:

$$CD_{AES(r_o=10)} = 10Sb_t + 11xor_t + 9MC_t + 10SR_t. \tag{13}$$

Next, we asses the computational cost (delay) of the proposed scheme. The delays introduced by the key generation technique and the proposed encryption process (for each frame symbol) are presented by the following equations:

$$CD_{(key.gen)} = h_t + xor_t, \tag{14}$$

$$CD_{(enc)} = En_t + U_t. \tag{15}$$

The proposed approach employs a single iteration structure and uses simple operations such as permutation or phase shuffling.

Considering the permutation scheme, the total Computational Delay (CD) that is required to encrypt one frame symbol is:

$$CD_{permutation} = \pi_t + U_t = 2\pi_t \tag{16}$$

In addition, it should be noted that the computational complexity of the proposed cipher scheme is linear ($O(N_m)$), where N_m is the number of modulation symbols in each frame symbol.

Based on the presented computational complexities, we can conclude that the AES scheme requires a higher computational delay than the proposed scheme, since the latter depends on just one round and one operation. Moreover, the proposed solution can use existing hardware optimization mechanisms for the permutation process to help reduce the required latency and resources even further. Regardless of any optimization, the proposed cipher scheme reduces the required execution time compared to any existing standard ciphers. This significant reduction is attained since a dynamic cryptographic concept is used.

Consequently, the proposed scheme demands less computational complexity than the AES standard cipher (128-bit secret key). The purpose of the proposed solution is to reinvent symmetric ciphers based on a dynamic key approach, to achieve the minimum possible overhead and better efficiency (latency and resources).

The computational complexity of current symmetric cryptographic algorithms, such as AES, is high as they require a high number of rounds and operations. Therefore, they require a longer execution time compared to the proposed scheme. This means that the proposed cipher scheme has less computational complexity and less execution time compared to AES. Less computational complexity means less execution time and, thus, less latency and minimum resource requirements for the ciphering/deciphering operations.

This is considered to be of high practical importance, especially for recent types of 5G networks where huge quantities of data are to be transmitted.

Finally, let us indicate that the proposed cipher scheme also reduces the hardware complexity.

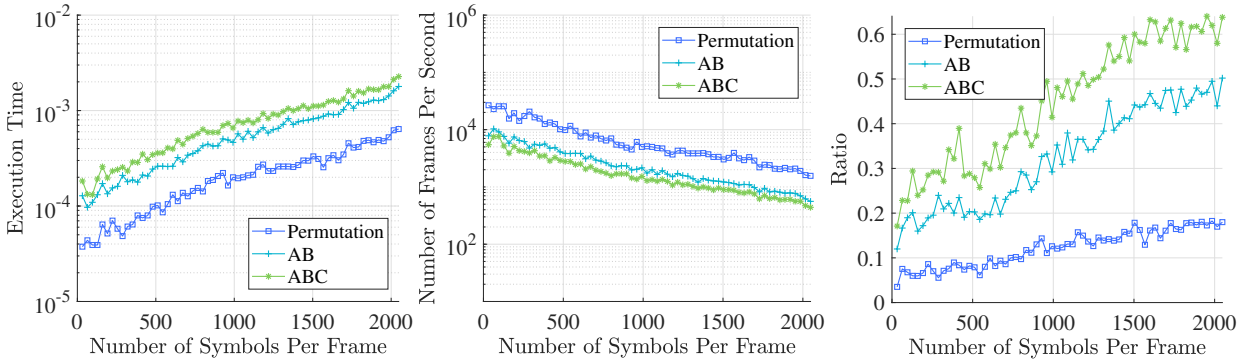
Table 9: Simulation Parameter table

Simulation parameter	**Value**
Signal to noise ration	30dB
Modulation order	QPSK
Number of frames	1000
Number of frames symbols (sub-frames)	128

7.2 Execution Time

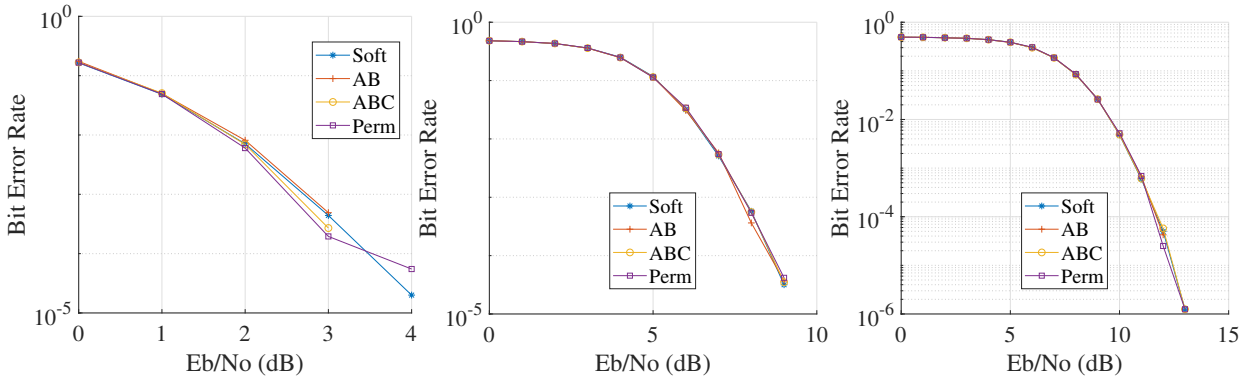
A low execution time reflects into low energy consumption, which is essential for resource-constrained devices. In this test, the average encryption time of frame symbols with varying sizes (32, 64, 128, 256, 512, 1024, and 2048) is computed. The hardware/software environment set-up includes: **Matlab R2018b simulator, Intel Core i7, 3 GHz CPU, 2 GB RAM Intel and the Microsoft Windows 10 operating system**. The considered simulation parameters are summarised in Table 9. Results in Fig. 14a reveal that the permutation cipher scheme requires the lowest execution time compared to the phase-amplitude scheme (“ABC"), which requires the highest execution time. Due to the

conversion and re-conversion operations, the phase encryption ("AB") scheme also requires more execution time compared to the permutation cipher scheme. Therefore, the permutation cipher scheme can be considered as the most efficient scheme that attains the right balance between security and performance.



(a) Execution Time (sec) (b) Number of encrypted symbols per second (c) Ratio

Figure 14: (a) The required execution time (sec) for the above chosen encryption schemes. (b) The number of encrypted frame symbols versus frame symbol size ($\log 2$), and (c) the ratio of execution time overhead (%) for different frame symbol lengths and using different ciphering schemes



(a) QPSK (b) 64-QAM (c) 256-QAM

Figure 15: The BER performance of selected encryption schemes versus E_b/N_0 using three modulations schemes: (a) QPSK, (b) 64-QAM and (c) 256-QAM modulation

7.3 Error Propagation

When designing a PLS cipher scheme, error tolerance must be taken into consideration to prevent any error from propagating to encrypted symbols, and prevent data corruption. Typically, noise and

interference are the main sources of error whereby a '0' bit is changed (flipped) to '1' bit and vice-versa. This is still a serious challenge in traditional cryptographic algorithms due to the trade-off that exists between the error propagation and the avalanche effect.

The proposed scheme ensures that any bit-error occurrence does not damage other modulation symbols, and the effect of erroneous bits is only limited to bits found at the same position in the plaintext and ciphertext.

Three cipher schemes are analyzed in terms of Bit Error Rate (BER). The number of frame symbols used in this test is equal to 10^4 with the following modulation techniques: QPSK, 64-QAM and 256-QAM.

Table 10: An evaluation of the proposed PLS scheme

Parameter	**Proposed Scheme**
Security	Proposed approach is based on a dynamic key dependent cipher structure, where each frame symbol is encrypted using variable cryptographic primitives
Delay	Low: each frame symbol is encrypted independently (scheme can be used in parallel)
Resources	Low: proposed cipher solution requires low computational complexity and, consequently, low resource requirements
Hardware complexity	Simple: one simple operation is used (substitution, permutation or masking)
Memory consumption	Low: encryption is realized at the OFDM symbol level
Error propagation	Low: low error propagation since encryption key is independent of ciphertext

As seen in Fig. 15a, the average BER curve of the input data (without encryption) is compared under different values of signal-to-noise power ratio (E_b/N_0), and for QPSK, 64-QAM and 256-QAM with the encrypted data frames. Based on the obtained results, BER reaches a minimum value of 4 dB for QPSK, 9 dB for 64-QAM, and 13 dB for 256-QAM. This difference is attributed to the modulation scheme itself since the distance between constellation symbols varies from one scheme to another. When the distance between constellation points decreases, any error demodulates into a completely different set of bits. Therefore, E_b/N_0 must be increased each time a higher order modulation scheme is used to achieve an acceptable BER. These results prove the absence of any error propagation when the proposed scheme is used, since the effect of erroneous bits is only restricted to the same position in the plaintext/ciphertext.

To justify the BER performance, a soft decision decoding that uses convolutional encoding is employed for the channel encoding/decoding process.

In summary, the results of the computational complexity, execution time and error propagation confirm that the proposed scheme is efficient and it achieves a good balance between performance and security (Table 10).

8 Conclusion

This paper presents a novel cipher scheme for NOMA downlink systems in order to achieve robust data confidentiality and privacy against internal and external attackers. The proposed cipher scheme is based on a simple dynamic key-dependent operation to secure NOMA at the frame symbol level. A key generation technique, which complements the proposed cipher scheme, is also presented. In particular, the random physical channel properties are used to generate a channel-based dynamic key, which is then used to derive the needed cipher primitives and update cipher primitives. The update cipher primitives change the cipher primitives used for encrypting data in a regular manner (for every input frame symbol), to overcome traditional attacks that rely on the relation between several encrypted data to recover the used key and, thus, the original data. The proposed scheme is general since any simple and efficient encryption operation can be used such as permutation or substitution. The main advantage behind utilizing physical layer parameters is reducing the number of iteration rounds. Specifically, using this approach, only a single round of simple operations is required to achieve the desired security level, unlike existing conventional cipher schemes which require multiple rounds. The proposed solution is analyzed and assessed in terms of different security metrics and properties, such as uniformity and sensitivity. According to the presented results, a high-security level is attained while maintaining an efficient system performance (low overhead and costs).

Acknowledgement

This paper was partially supported by funds from 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").

References

[1] J. Zeng, T. Lv *et al.*, "Investigation on evolving single-carrier NOMA into multi-carrier NOMA in 5G," *IEEE Access*, vol. 6, pp. 48 268–48 288, 2018.

[2] I. Baig *et al.*, "On the PAPR reduction: A novel filtering based hadamard transform precoded uplink MC-NOMA scheme for 5G cellular networks," in *Proc. IEEE International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2018, pp. 1–4.

[3] C. Chen, W. Zhong, H. Yang, and P. Du, "On the performance of MIMO-NOMA-based visible light communication systems," *IEEE Photonics Technology Letters*, vol. 30, no. 4, pp. 307–310, 2017.

[4] J. Datta and H. Lin, "Detection of uplink NOMA systems using joint SIC and cyclic FRESH filtering," in *Proc. IEEE Wireless and Optical Communication Conference (WOCC)*. IEEE, 2018, pp. 1–4.

[5] T. Zhao, G. Li, G. Zhang, and C. Zhang, "Security-enhanced user pairing for MISO-NOMA downlink transmission," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[6] H. Bao, C. Zhang, L. Wu, and M. Li, "Design of physical layer secure transmission scheme based on SWIPT NOMA systems," in *Proc. IEEE International Conference on Communication Technology (ICCT)*. IEEE, 2017, pp. 6–9.

[7] H. Noura, R. Melki, A. Chehab, and M. Mansour, "A physical encryption scheme for low-power wireless M2M devices: a dynamic key approach," *Mobile Networks and Applications*, pp. 1–17, 2018.

[8] S. Islam *et al.*, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 721–742, 2016.

[9] M. Le *et al.*, "On information-theoretic limits of code-domain NOMA for 5G," *IET Communications*, vol. 12, no. 15, pp. 1864–1871, 2018.

[10] S. Islam *et al.*, "NOMA in 5G systems: Exciting possibilities for enhancing spectral efficiency," *arXiv preprint arXiv:1706.08215*, 2017.

[11] M. Aldababsa *et al.*, "A tutorial on nonorthogonal multiple access for 5G and beyond," *Wireless Communications and Mobile Computing*, 2018.

[12] B. Da-Silva *et al.*, "A multistage method for SCMA codebook design based on MDS codes," *IEEE wireless communications letters*, vol. 8, no. 6, pp. 1524–1527, 2019.

[13] R. Kizilirmak and H. Bizaki, "Non-orthogonal multiple access (NOMA) for 5G networks," *Towards 5G Wireless Networks-A Physical Layer Perspective*, pp. 83–98, 2016.

[14] H. Furqan *et al.*, "Physical layer security for NOMA: Requirements, merits, challenges, and recommendations," *arXiv preprint arXiv:1905.05064*, 2019.

[15] H. Zhang *et al.*, "Heterogeneous ultra dense networks: Part 2," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 12–13, 2018.

[16] H. Noura, R. Melki, A. Chehab, M. Mansour, and S. Martin, "Efficient and secure physical encryption scheme for low-power wireless M2M devices," in *proc. IEEE International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 1267–1272.

[17] S. Cioni *et al.*, "On the satellite role in the era of 5G massive machine type communications," *IEEE Network*, vol. 32, no. 5, pp. 54–61, 2018.

[18] R. Melki, H. Noura, M. Mansour, and A. Chehab, "A survey on OFDM physical layer security," *Physical Communication*, vol. 32, pp. 1–30, 2019.

[19] H. Tayakout, I. Dayoub, K. Ghanem, and H. Bousbia-Salah, "Automatic modulation classification for d-stbc cooperative relaying networks," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 780–783, 2018.

[20] Q. Le, V. Bao, and B. An, "Full-duplex distributed switch-and-stay energy harvesting selection relaying networks with imperfect CSI: Design and outage analysis," *Journal of Communications and Networks*, vol. 20, no. 1, pp. 29–46, 2018.

[21] M. Pajovic, T. Akino, and P. Orlik, "Localization using millimeter wave communication signals," Sep. 24 2019, uS Patent App. 10/425,910.

[22] P. Ferreira *et al.*, "Multiobjective reinforcement learning for cognitive satellite communications using deep neural network ensembles," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 5, pp. 1030–1041, 2018.

[23] R. Melki, H. Noura, M. Mansour, and A. Chehab, "An efficient OFDM-based encryption scheme using a dynamic key approach," *IEEE Internet of Things Journal*, 2018.

[24] C. Biton and S. Arnon, "Improved multiple access resource allocation in visible light communication systems," *Optics Communications*, vol. 424, pp. 98–102, 2018.

[25] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[26] M. Liaqat *et al.*, "Power-domain non orthogonal multiple access (PD-NOMA) in cooperative networks: an overview," *Wireless Networks*, vol. 26, no. 1, pp. 181–203, 2020.

[27] Y. Liu, Z. Qin, and Z. Ding, "Artificial intelligence (AI) enabled NOMA," in *Non-Orthogonal Multiple Access for Massive Connectivity*. Springer, 2020, pp. 89–94.

[28] G. Satrya and Y. Shin, "Enhancing security of SIC algorithm on non-orthogonal multiple access (NOMA) based systems," *Physical Communication*, vol. 33, pp. 16–25, 2019.

[29] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1670–1683, June 2019.

[30] M. Abolpour, M. Mirmohseni, and M. Aref, "Outage performance in secure cooperative NOMA," in *Proc. IEEE Iran Workshop on Communication and Information Theory (IWCIT)*. IEEE, 2019, pp. 1–6.

[31] Y. Alsaba, C. Leow, and S. Abdul-Rahim, "Null-steering beamforming for enhancing the physical layer security of non-orthogonal multiple access system," *IEEE Access*, vol. 7, pp. 11 397–11 409, 2019.

[32] B. Zheng *et al.*, "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1426–1440, July 2018.

[33] Z. Xiang *et al.*, "Physical layer security in cognitive radio inspired NOMA network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 700–714, 2019.

[34] F. Zhou *et al.*, "Enhancing PHY security of MISO NOMA SWIPT systems with a practical non-linear EH model," in *Proc. IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2018, pp. 1–6.

[35] B. Zheng, F. Chen, M. Wen, Q. Li, Y. Liu, and F. Ji, "Secure NOMA based cooperative networks with rate-splitting source and full-duplex relay," in *Proc. IEEE International Symposium on Wireless Communication Systems (ISWCS)*, Aug 2018, pp. 1–5.

[36] M. Zeng, N. Nguyen, O. Dobre, and H. Poor, "Securing downlink massive MIMO-NOMA networks with artificial noise," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 685–699, June 2019.

[37] Y. Feng *et al.*, "Beamforming design and power allocation for secure transmission with NOMA," *IEEE Transactions on Wireless Communications*, vol. 18, no. 5, pp. 2639–2651, May 2019.

[38] J. Chen, L. Yang, and M. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[39] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, April 2018.

[40] F. Jiang, G. Huang, W. Liu, and C. Sun, "Adaptive power allocation for D2D assisted cooperative relaying system with NOMA," in *Proc. IEEE/CIC International Conference on Communications in China (ICCC)*, Aug 2018, pp. 676–681.

[41] L. Lei *et al.*, "Power and load optimization in interference-coupled non-orthogonal multiple access networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec 2018, pp. 1–6.

[42] L. You *et al.*, "Resource optimization with load coupling in multi-cell NOMA," *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4735–4749, July 2018.

[43] B. Su, Q. Ni, and B. He, "Robust transmit designs for secrecy rate constrained MISO NOMA system," in *Proc. IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2018, pp. 1–5.

[44] A. Islam, M. Uddin, M. Kader, and S. Shin, "Blockchain based secure data handover scheme in non-orthogonal multiple access," in *Proc. IEEE International Conference on Wireless and Telematics (ICWT)*, July 2018, pp. 1–5.

[45] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, and M. Mansour, "One round cipher algorithm for multimedia iot devices," *Multimedia Tools and Applications*, pp. 1–31, 2018.

[46] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.