University of Mississippi

eGrove

Faculty and Student Publications

Engineering, School of

1-1-2020

Revisiting Lightweight Encryption for IoT Applications: Error Performance and Throughput in Wireless Fading Channels with and without Coding

Yazid M. Khattabi
University of Jordan

Mustafa M. Matalgah
University of Mississippi

Mohammed M. Olama
Oak Ridge National Laboratory

Follow this and additional works at: https://egrove.olemiss.edu/engineering_facpubs

Part of the Biomedical Engineering and Bioengineering Commons, Chemical Engineering Commons, Civil and Environmental Engineering Commons, Computer Engineering Commons, Electrical and Computer Engineering Commons, Geological Engineering Commons, and the Mechanical Engineering Commons

Recommended Citation

Khattabi, Y. M., Matalgah, M. M., & Olama, M. M. (2020). Revisiting Lightweight Encryption for IoT Applications: Error Performance and Throughput in Wireless Fading Channels With and Without Coding. IEEE Access, 8, 13429–13443. https://doi.org/10.1109/ACCESS.2020.2966596

This Article is brought to you for free and open access by the Engineering, School of at eGrove. It has been accepted for inclusion in Faculty and Student Publications by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 18, 2019, accepted January 2, 2020, date of publication January 14, 2020, date of current version January 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2966596

Revisiting Lightweight Encryption for IoT Applications: Error Performance and Throughput in Wireless Fading Channels With and Without Coding

YAZID M. KHATTABI[1], (Member, IEEE), MUSTAFA M. MATALGAH[2], (Senior Member, IEEE), AND MOHAMMED M. OLAMA[3], (Senior Member, IEEE)

[1]Department of Electrical Engineering, The University of Jordan, Amman 11942, Jordan
[2]Department of Electrical Engineering, University of Mississippi, University, MS 38677, USA
[3]Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA

Corresponding author: Mustafa M. Matalgah (mustafa@olemiss.edu)

This work was supported in part by the Laboratory Directed Research and Development Program of Oak Ridge National Laboratory.

ABSTRACT Employing heavy conventional encryption algorithms in communications suffers from added overhead and processing time delay; and in wireless communications, in particular, suffers from severe performance deterioration (avalanche effect) due to fading. Consequently, a tremendous reduction in data throughput and increase in complexity and time delay may occur especially when information traverse resource-limited devices as in Internet-of-Things (IoT) applications. To overcome these drawbacks, efficient lightweight encryption algorithms have been recently proposed in literature. One of those, that is of particular interest, requires using conventional encryption only for the first block of data in a given frame being transmitted. All the information in the remaining blocks is transmitted securely without the need for using heavy conventional encryption. Unlike the conventional encryption algorithms, this particular algorithm achieves lower overhead/complexity and higher data throughput. Assuming the additive white Gaussian noise (AWGN) channel, the performance of the lightweight encryption algorithm under study had been evaluated in literature in terms of throughput under the assumption that the first block, that undergoes conventional encryption, is free of error, which is practically unfeasible. In this paper, we consider the AWGN channel with Rayleigh fading and assume that the signal experiences a certain channel bit error probability and investigate the performance of the lightweight encryption algorithm under study in terms of bit error probability and throughput. We derive analytical expressions for these performance metrics considering modulated signals with and without coding. In addition, we propose an extension to the lightweight encryption algorithm under study by further enhancing its security level without significantly affecting the overhead size and processing time. Via numerical results we show the superiority of the lightweight encryption algorithm under study over the conventional encryption algorithms (like the AES) and the lightweight encryption algorithms proposed in literature in terms of error and throughput performance.

INDEX TERMS Lightweight encryption, security, wireless fading channels, AWGN channel, error performance, throughput, error correction coding.

I. INTRODUCTION

Tth wireless communication link in general is insecure and open to intruders. Hence, it is vulnerable to various types of attacks where an eavesdropper can easily intercept a communication signal, alter it, and forward it to the destination or resend it back to the source. Consequently, none of the confidentiality, integrity, or authenticity of the message is preserved while traversing the wireless medium. It is undisputable that the last two decades have witnessed a tremendous increase in number of wireless applications offered over the Internet and in the development of standards for wireless

The associate editor coordinating the review of this manuscript and approving it for publication was Congduan Li.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

packet service; among those are the recently developed technologies such as 5G, Internet-of-Things (IoT), and cloud computing applications just to name a few. Given these large technologies advancements, demand for wireless content has been extremely increasing, and hence, wireless network security based on encryption has become crucial to satisfy end-to-end confidential communications. However, conventional encryption algorithms had been designed based on the fact that security against an adversary attack is the only main criterion with the objective that the encrypted data (i.e., the cipher) is made to satisfy several properties including the avalanche effect [1], [2], and [3].

The avalanche criterion is a desirable property of any encryption algorithm from the security point of view. It requires that a single bit change to the plaintext or the key must result in significant and random-looking changes to the ciphertext and vice versa; and hence a highly secured algorithm is obtained. In general, if an intruder complements a single bit at the input to the decryption device then an average of one half of the decrypted bits should change, which produces a highly secured and reliable data transmission assuming that the communication link is characterized with perfect channel conditions. Particularly, in a communication system with perfect channel conditions the encrypted data is received at the destination with no error, and hence it can be perfectly decrypted at the receiver to recover the exact plaintext that was encrypted at the transmitter. This property does in fact significantly reduce the keyspace search by the cryptanalyst in order to guarantee that there will not be any noticeable resemblance between two ciphertexts obtained by applying two neighboring keys for encrypting the same plaintext. On the other hand, these same conventional encryption algorithms do not take into account wireless network characteristics such as random bit errors due to noise or interference and burst errors due to fading. Due to these random bit errors, the avalanche effect that makes a block cipher secure also causes it to be sensitive to bit errors.

In [3] and [4], the authors showed that secret-key encryption systems multiply bit errors by more than an order of magnitude. As a result, systems that use conventional encryption algorithms degrade quality of service (QoS) in exchange for end-to-end data confidentiality. Given the large amount of increase in wireless technologies deployment, the vast majority of the communication contents traverses a wireless link between a source and destination, and hence, the need for developing new encryption algorithms that surmount the effect of the avalanche criterion is becoming vital. This problem has received a great deal of attention in recent years and motivated researchers in analyzing current standard encryption algorithms in terms of bit error rate, throughput, complexity, and energy efficiency in a wireless communication environment and proposing new encryption algorithms that alleviate the avalanche effect (see e.g., [3]–[13]). The author in [3] quantitatively analyzed and characterized the trade-off between QoS and confidentiality and proposed solutions to mitigate this trade-off. Another trade-off between security and throughput in encryption-based wireless systems was studied in [5]. The authors in [5] also proposed a technique they called *opportunistic encryption* that uses channel opportunities, based on acceptable signal to noise ratio as a performance measure, to maximize the throughput subject to desired security constraints. Simulation results showed some improvement in the performance as compared to conventional approaches. In [6], [8], [12], [13], the authors proposed new encryption algorithms with improved error performance, reduced computational complexity, and improved throughput in a wireless fading environment. In [11], the authors developed an optimization framework for trading-off between security and throughput in a wireless environment based on the improved error performance algorithms reported in [6], [13]. Computational complexity and energy efficiency analyses for a class of symmetric crypto-systems are reported in [7], [9], [10].

From research findings in literature, it is becoming unarguable that conventional encryption requires extra large amount of bandwidth in wireless environment because of the added packet overhead and the performance deterioration due to fades in wireless channels (avalanche effect); hence tremendously reducing the effective bandwidth utilization in the wireless spectrum that is already crowded. This is in addition to the delay caused by the processing time required by the encryption/decryption algorithms at the source/destination, respectively. Although, conventional cryptography of the plaintext achieves security and privacy, all these drawbacks add to large reduction in the effective transmission data rate (throughput) in a wireless environment. Moreover, performance deterioration due to fades in wireless channels may in some extreme conditions make it almost impossible to decrypt the data at the destination without powerful error-correction coding techniques, which in fact will add more processing delay.

IoT-enabled devices are among the communication entities that are not equipped with processors that can handle algorithms that require highly complex computations and large time delays. IoT devices used in applications such as smart homes, smart buildings, smart cities, smart healthcare, smart grid, transportation, vehicle-to-everything (V2X) communication, etc., are mainly wireless sensors that communicate with servers. Protecting information captured by these sensors is a crucial factor because the transmission channel from the sensor to the database server could be vulnerable to attacks especially in a wireless environment. However, conventional standard encryption algorithms, such as the Advanced Encryption Standard (AES), cannot be used in IoT applications due to their drawbacks (as mentioned earlier) that do not fit the limited memory space and computational capabilities of IoT devices [14]. To encounter these challenges, lightweight encryption methods have been proposed in literature to be implemented on these resource-constrained devices [15]–[25]. In [15], a lightweight cellular automata-based encryption algorithm has been proposed for IoT applications, where sensors' data is encrypted at the perception layer and decrypted at the gateway's network layer. As compared to classical encryption algorithms like the data encryption standard (DES), the proposed algorithm in [15] has shown higher efficiency in terms of running time and implementation complexity. In [16], a modification to the lightweight key-policy attribute-based encryption (KP-ABE) model has been proposed to improve its security level and efficiency such that it would be more suitable for IoT applications. Reported results in [16] have shown that the enhanced KP-ABE model remarkably offers low running time as compared to other similar encryption algorithms. In [17], an enhanced version of the AES encryption algorithm in terms of running time and energy consumption has been presented. Obtained results in [17] have confirmed it is fair to claim that enhanced algorithm is lightweight and efficient for voice applications in wireless systems. In [18], a hybrid lightweight encryption algorithm for IoT networks has been proposed. The hybrid algorithm employs both the symmetric and asymmetric encryption methods in a way that results in low execution time in comparison with the AES. In [19], a lightweight encryption algorithm for surveillance videos has been proposed. The proposed algorithm is cellular automata based and requires encrypting the privacy-sensitive regions instead of encrypting the entire video stream. In comparison with classical encryption algorithms, the proposed algorithm has proven its effectiveness especially for real time applications. For other promising IoT applications such as smart buildings, smart grid infrastructure, and wireless body area networks, efficient lightweight encryption algorithms have been proposed in [20], [22], and [24], respectively.

Among the relevant works in literature, the analysis in [25] is of particular interest as it requires using conventional encryption only for the first block of data in a given frame (or superframe) being transmitted. The size of this data block is determined by the conventional encryption algorithm to be applied on this first block. All the remaining information in the frame is transmitted securely over the wireless channel without the need for using heavy conventional encryption. Unlike the conventional and opportunistic encryption algorithms, the proposed algorithm in [25] has been shown to achieve lower overhead/complexity and higher data transmission rates. The security of the introduced scheme in [25] may not be as good as the conventional techniques. However, the scheme can still be useful in applications when it is preferable to attain high throughput with moderate security such IoT-enabled devices as explained above. Nevertheless, two issues in the work of [25] has to be addressed. First, assuming the additive white Gaussian noise (AWGN) channel model, the performance of the lightweight encryption algorithm in [25] has been evaluated in terms of throughput under the assumption that the first block, that undergoes conventional encryption, is free of error, which is practically unfeasible. Second, the security level of the lightweight encryption model could be further enhanced.

Thus, the contribution of this work is two-fold. First, we analytically examine the performance of the lightweight encryption model under study considering the AWGN channel with Rayleigh fading and assume that all data in the frame, including the first block, experience some error with certain probability and investigate its performance in terms of bit error probability as well as throughput. Specifically, we derive novel analytical expressions for these performance metrics considering both cases of with and without data channel encoding. Second, we propose to enhance the security level of the lightweight encryption algorithm in [25]. Specifically, we propose to add a new security process box to be implemented at the transmitting side and to reverse it at the receiving side. The impressive side of such improvement is that (i) it does not come at the cost of adding significant overhead size or processing delay (i.e., the improved algorithm is still lightweight as compared to classical encryption algorithms such as AES); (ii) it offers the same improved error rate and throughput performance as, yet more secure than, that of the original lightweight algorithm in [25]. Provided numerical results under different channel and coding scenarios show that the algorithm under study offers enhanced performance as compared to the conventional encryption algorithm AES and the lightweight encryption algorithms proposed in literature (like the one in [26]).

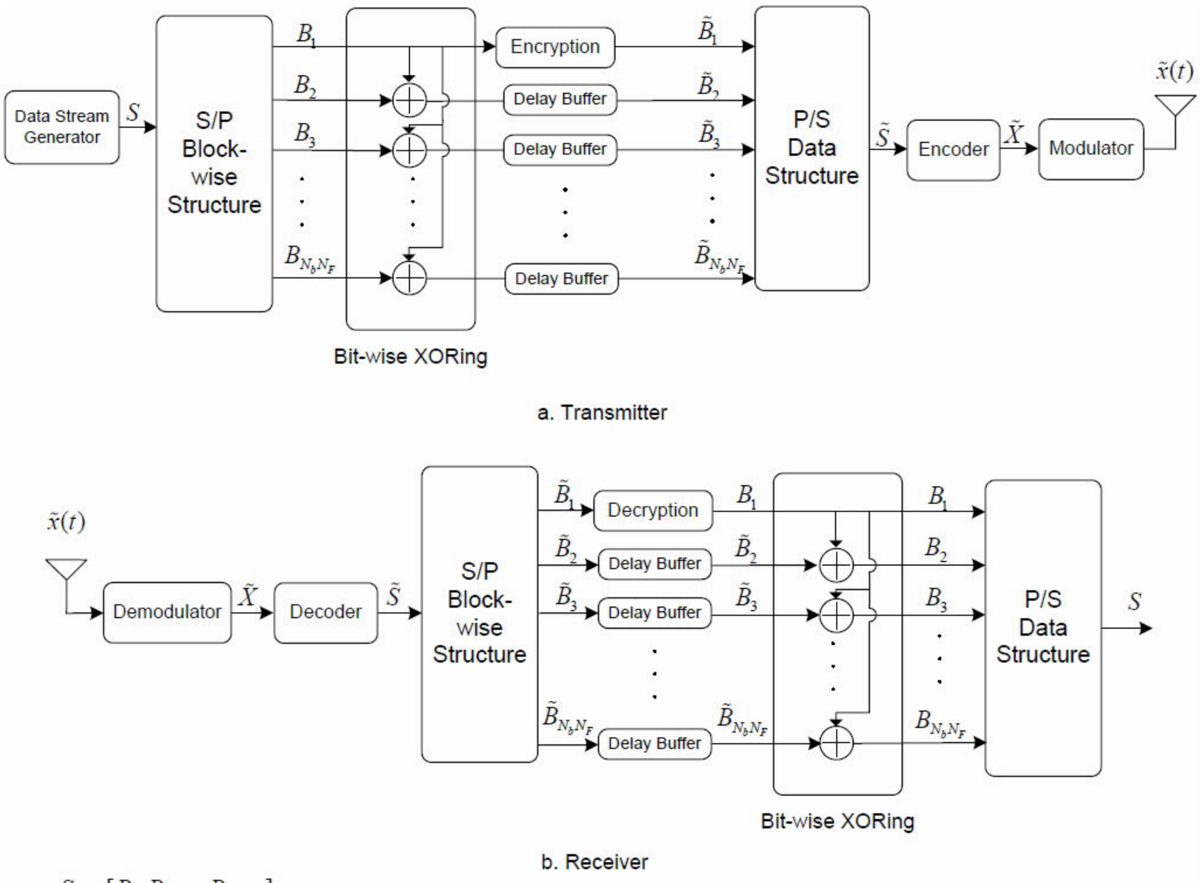
The remainder of this paper is organized as follows. Section II presents a review of the algorithm structure of the lightweight encryption model proposed in [25]. Performance analyses of this lightweight encryption model, in terms of probability of bit error and throughput, are given in Section III and Section IV, respectively. The proposed security enhancement on the lightweight encryption model under study is given in Section V. Numerical results are presented in Section VI. Finally, some conclusions are drawn in Section VII.

II. REVIEW OF LIGHTWEIGHT ENCRYPTION MODEL PROPOSED IN [25]

A. TRANSMITTER AND RECEIVER STRUCTURES

A conceptual structure for the transceiver system that employs the light encryption algorithm reported in [25] is shown in Fig. 1. The transmitter structure is depicted in Fig. 1.a, where the incoming serial data stream (S in bits) is mapped into parallel data blocks, each with a common pre-specified block length (β_l).[1] The first block undergoes a proper encryption alogorithm satisfying a certain security level. All the remaining blocks are arranged systematically and enter a bit-wise XOR operation with the first block (before encryption, i.e., plaintext), as can be seen from the figure. The delay buffers are used just to control the data flow into the P/S convertor so the serial data are produced systematically. Next, the data is mapped back into a serial format to be encoded before transmission (both source and

[1] The algorithm requires that the block size β_l be determined by the encryption algorithm that will be applied only to the first block.



$$S = [B_1, B_2, \ldots, B_{N_bN_F}]$$

$$B_k = [b_{1,k}, b_{2,k}, \ldots, b_{\beta_l,k}], k = 1, 2, 3, \ldots, N_bN_F$$

$$\tilde{B}_1 = E_k[B_1]$$

$$\tilde{B}_k = B_1 \oplus B_k, \ k = 2, 3, \ldots, N_bN_F$$

FIGURE 1. **Transmitter and receiver structures.**

channel encoding) to enhance transmission reliability. The data stream is then modulated using any digital modulation technique in order to be suitable for transmission. Without loss of generality, in this paper we consider the binary phase shift keying (BPSK) modulation scheme and the analysis can be generalized to any other higher-order modulation. The receiver structure, as can be seen in Fig. 1.b, completely reverses all the operations performed at the transmitter. Also, at the receiver side, only the first block is needed to be decrypted using an appropriate conventional decryption algorithm and the decryption key, whereas all the other blocks are bit-wise XORed with the first decrypted block (plaintext). As a result, all the data frame is transmitted securely by only performing encryption on the first amount of data (B_1 in Fig. 1) within a frame/superframe while transmitting the remaining blocks after XORing each with the hidden plaintext block B_1. It should be obvious to the reader that the operations performed by the bank of XOR gates along with the S/P and P/S blocks, in Fig. 1, can be practically implemented by a shift-register, one XOR gate, and a switch. The structure shown in the figure is used to just simplify the understanding of the concept.

B. THE ALGORITHM

Before we outline the lightweight encryption algorithm proposed in [25], we first define the data structure to be used in the algorithm. Data sequence is assumed to be composed of N superframes. Each superframe contains N_F frames, and each frame consists of N_b blocks, each of $K = \beta_l$ bits size, as can be seen in Fig. 2. The transmission algorithm is detailed in the text structure in Algorithm 1. The notations used in Algorithm 1 are defined as follows: B_j : the j^{th} block of data (plaintext); $\tilde{B}_j$: the j^{th} block of the encrypted data (ciphertext); β_l : block length in bits; N_F : number of frames within a superframe; N_b : number of blocks within a frame; $b_{i,j}$: the i^{th} bit of the j^{th} block of the data (plaintext);

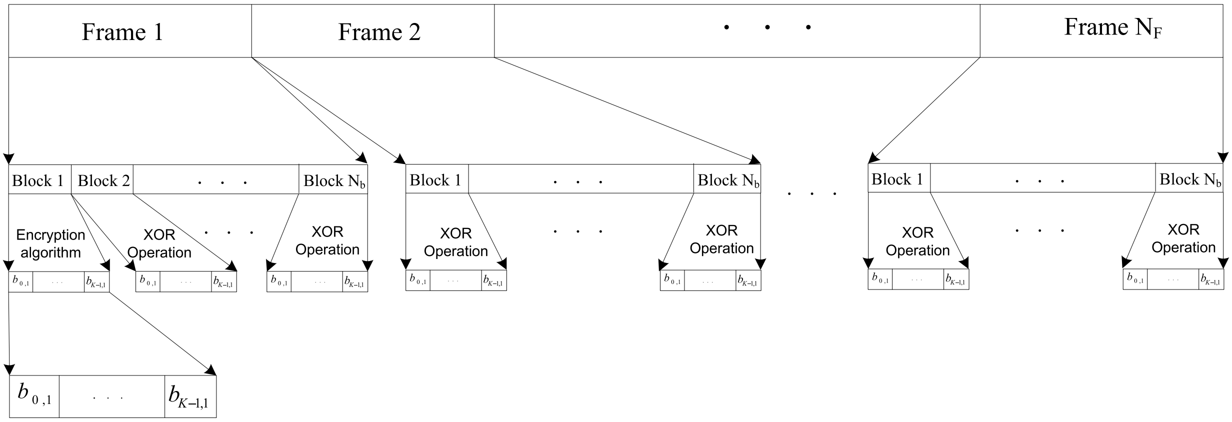
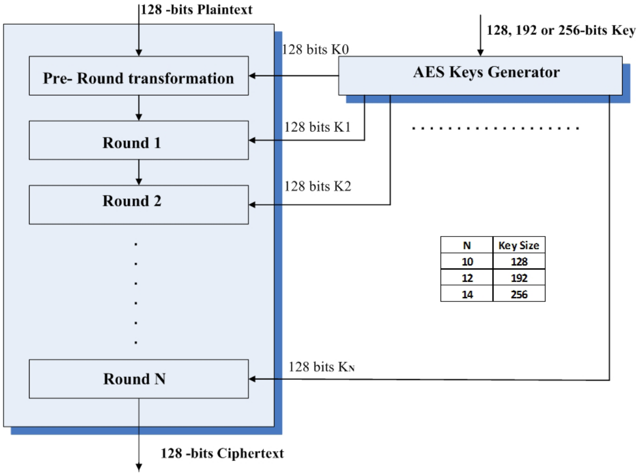


FIGURE 2. Superframe structure.

and $\tilde{b}_{i,j}$: the i^{th} bit of the j^{th} block of the encrypted data (ciphertext). As it is clear from the steps in Algorithm 1, we first encrypt the first block, B_1, with a highly immune standard conventional encryption algorithm, where in this work we adopt the AES.[2] Following this step, the remaining of the $N_b N_F - 1$ plaintext blocks will not undergo conventional encryption, but a bit-wise XOR operation is performed between each of these plaintext blocks and the plaintext of the first block, which is unknown to intruders, and hence the resultant blocks will be transmitted to the destination with same security level as the first block. Perceptively speaking, the first block will not be recovered without performing the decryption process, which is assumed to be very immune for cryptanalysis, and therefore the other blocks will not be detected by the intruders since the plaintext of the first block is required to undo the XOR operation. This latter operation can be performed to reveal all the plaintexts only after decrypting the first block, B_1, at the receiver.

By performing the proposed mechanism following the steps provided in Algorithm 1, the whole resultant data stream will then be secure since the data will not be recovered by any intruder without breaking the first cipher $\tilde{B}_1$ that is encrypted using AES. Security and reliability of transmission can be further enhanced if Algorithm 1 is executed every one superframe (N_F frames) or multiple of superframes using a new encryption key.



N	Key Size
10	128
12	192
14	256

FIGURE 3. AES general architecture.

III. BER ANALYSIS OF LIGHTWEIGHT ENCRYPTION MODEL PROPOSED IN [25]

We first describe the encryption ratio (β_c) introduced in [25], as a figure of merit to be used in the performance analysis in this paper, which is defined as the ratio of the overall length of ciphertext using the XOR operation to the length of ciphertext using conventional algorithms; i.e., $\beta_c = \frac{(N_F N_b - 1)\beta_l}{\beta_l} = (N_F N_b - 1)$ where N_F, N_b, and β_l are as defined before. This parameter reveals the amount of overhead reduction when using this particular algorithm. As a result, as the value of β_c increases, the overhead decreases for a given superframe of data and hence the throughput increases.

A. ERROR ANALYSIS WITHOUT DATA ENCODING

In this subsection, we analyze the overall superframe average bit error rate (BER) performance for the encryption algorithm under study assuming BPSK transmission over AWGN channel model without data error correction encoding. We also compare this BER with the one for the conventional encryption algorithm (i.e., all of the superframe blocks are assumed

[2] The AES cipher algorithm is a known standard algorithm that is very immune to adversary attack by intruders such as a brute force attacker. The encryption key is assumed to be known only to the destination node where the cipher message of the first block is received and decrypted to convey the plaintext. The AES cipher requires a 128 block size and a 128/192/256 key size that satisfies the entropy condition for the key size. The general design of the AES has pre-round transformation (initial stage), $R-$rounds, key expansion, and a final stage. The number of rounds is determined by the key size. Particularly, the AES uses 10, 12, and 14 rounds for key sizes of 128, 192, and 256, respectively. The number of processing cycles for each operation (AND, OR, Exclusive OR (XOR), and SHIFT) varies based on the number of rounds included in the encryption algorithm as a result of different keys adopted. Also, the number of overhead processing cycles (PC) in the decryption is larger than the number of PC used in the encryption. The general architecture of AES is shown in Fig. 3.

```
Input: Data stream as plaintext
Output: Data stream as ciphertext
Divide the data sequence into $N$ superframes;
foreach $N_i$ superframe $SF_i$, $i = 1, \ldots, N$, to be sent do
    Divide each superframe into $N_F$ frames;
    Divide the frame $(F_k)$, $k = 1, \ldots, N_F$, into $N_b$
    blocks with block size of $K = \beta_l$;
    Encrypt the first block $B_1$ with an appropriate
    encryption algorithm, i.e., $\tilde{B}_1 = E_k[B_1]$ foreach of
    the remaining blocks $B_j$, $j \in \{2, 3, \ldots, N_bN_F\}$ do
        $\tilde{b}_{i,j} = b_{i,j} \oplus b_{i,1}$, $i \in \{0, 1, \ldots, K-1\}$;
        Generate the cipher blocks as
        $\tilde{B}_j = [\tilde{b}_{0,j}, \ldots, \tilde{b}_{K-1,j}]$ ;
    end
    Generate the cipher frame as
    $\tilde{S} = [\tilde{B}_1, \tilde{B}_2, \cdots, \tilde{B}_{N_bN_F}]$;
end
Generate the cipher superframe accordingly. Repeat for
other superframes;
```

Algorithm 1 Generating Lightweight Ciphertext Based on Proposed Algorithm in [25]

to be encrypted via a conventional encryption algorithm such as AES). Our target is to find the superframe average BER at the output of the receiver P/S convertor. This is possible by tracking the bits propagation through the different stages in the receiver. As shown in Fig. 1, at the output of the demodulator (before decryption), each detected bit of the received superframe has BER caused by the noise in the channel, say P_{e_G}, which is, for BPSK modulation [27, Eq. (5.2-5)], given as

$$P_{e_G} = Q\left(\sqrt{2\gamma_b}\right) \tag{1}$$

where $\gamma_b = \frac{E_b}{N_o}$ is the average signal-to-noise power ratio (SNR) per bit with per-bit average energy of E_b and white Gaussian noise with variance of $\frac{N_o}{2}$. After that, these detected bits pass through the S/P convertor in order to divide the detected superframe into its blocks $\tilde{B}_1, \tilde{B}_2, \cdots, \tilde{B}_{N_bN_F}$. Among all of these blocks, only $\tilde{B}_1$ ciphertext block is decrypted using conventional decryption algorithm and a decryption key to obtain the plaintext block B_1, whereas each of the remaining blocks $(\tilde{B}_2, \tilde{B}_3, \cdots, \tilde{B}_{N_bN_F})$ is bit-wise XORed with the first decrypted block B_1 to obtain the remaining plaintext blocks $B_2, B_3, \cdots, B_{N_bN_F}$. Since the first block, B_1, is encrypted differently (i.e., using conventional encryption) than the remaining blocks, it is expected to experience different BER (with avalanche [1], [2], [4], [28]), say P_{e_E}, while the remaining blocks, $B_2, B_3, \cdots, B_{N_bN_F}$, will experience equal BER, say $P_{e_{XOR}}$, which is quantitatively different from P_{e_E}. The BER associated with the decrypted block B_1, P_{e_E}, which is the BER at the output of the decrypter (caused by decryption avalanche effect) has been derived in [28] in terms of the BER at the input of the decrypter (caused by channel noise and fades), which is given by

$$P_{e_E} = 0.5\left(1 - [1 - P_{e_G}]^{\beta_l}\right). \tag{2}$$

In order to derive $P_{e_{XOR}}$, we first consider the *kth* block B_k where $k = 2, 3, \ldots, N_bN_F$. The *lth* bit in B_k, say $b_{l,k}$, results from XORing the *lth* bit of B_1, i.e. $b_{l,1}$, with the *lth* bit of $\tilde{B}_k$, $\tilde{b}_{l,k}$ for $k = 2, 3, \ldots, N_bN_F$. Consequently, $b_{l,k}$ is decrypted correctly, with bit correct probability, say $P_{c_{XOR}}$, if and only if both of $b_{l,1}$ and $\tilde{b}_{l,k}$, for $k = 2, 3, \ldots, N_bN_F$, are correct or both are in error. By defining the following events: $A = \{$both of $b_{l,1}$ and $\tilde{b}_{l,k}$ are correct$\}$, $B = \{$both of $b_{l,1}$ and $\tilde{b}_{l,k}$ are in error$\}$, $A_1 = \{b_{l,1}$ is correct$\}$, $A_2 = \{\tilde{b}_{l,k}$ is correct$\}$, $A_3 = \{b_{l,1}$ is in error$\}$ and $A_4 = \{\tilde{b}_{l,k}$ is in error$\}$, we can write

$$\begin{aligned} P_{c_{XOR}} &= Pr\{A \cup B\} = Pr\{A\} + Pr\{B\} - Pr\{A \cap B\} \\ &= Pr\{A_1 \cap A_2\} + Pr\{A_3 \cap A_4\} - 0 \\ &= Pr\{A_1\}Pr\{A_2\} + Pr\{A_3\}Pr\{A_4\} \\ &= (1 - P_{e_E})(1 - P_{e_G}) + P_{e_E}P_{e_G}. \end{aligned} \tag{3}$$

And hence,

$$P_{e_{XOR}} = 1 - P_{c_{XOR}} = P_{e_G} + P_{e_E} - 2P_{e_G}P_{e_E}. \tag{4}$$

Now, the superframe average BER for the algorithm under study can be given as

$$\begin{aligned} P_{e_{proposed}} &= \frac{P_{e_E} + (N_bN_F - 1)P_{e_{XOR}}}{N_bN_F} \\ &= \frac{P_{e_E} + \beta_c P_{e_{XOR}}}{\beta_c + 1}. \end{aligned} \tag{5}$$

It should be noted that if heavy conventional encryption was used throughout the whole blocks, then the superframe average BER in (5) reduces, as expected, to

$$P_{e_{conv}} = \frac{P_{e_E} + (N_bN_F - 1)P_{e_E}}{N_bN_F} = P_{e_E}. \tag{6}$$

B. ERROR ANALYSIS WITH DATA ENCODING

In this subsection, in order to investigate the effect of data error correction encoding on BER analysis, we assume that the encoder/decoder pair shown in Fig. 1 is active and two types of error correction coding techniques are considered, namely, the Hamming encoder and the convolutional encoder. Hamming code [29, Ch. 4] belongs to the linear block codes (LBC) family and it is parameterized by an integer $\ell \geq 2$. For (n, k) Hamming code, $n = 2^\ell - 1$ is the encoder output codeword length, $k = 2^\ell - \ell - 1$ is the encoder information sequence input length, and $R_c = \frac{k}{n}$ is the coding rate. The error correction capability factor t for the Hamming encoder is 1, and hence, it has a minimum distance d_{min} of 3 [29, Ch. 4]. Convolutional codes [29, Ch. 11] differ from LBC codes in that the encoder contains memory. This means that the encoder output at any given time unit depends on the input at this time unit and on some number of previous inputs. A convolutional code is defined by three parameters, K the number of inputs, N the number of outputs and m the memory order, and hence, it can be described either as: (N, K, m) *convolutional code* or as *a rate* $R = \frac{K}{N}$ *convolutional code* *with memory order m*. Furthermore, the code rate of the convolutional code is given as $R_c = \frac{k}{n} = \frac{h}{h+m}R = \frac{h}{h+m}\frac{K}{N}$ where h is the length of information sequence at any input of the code [29, pp. 485-486]. If $h \gg m$, then $\frac{h}{h+m} \approx 1$, and hence, $R_c \approx R$. In addition, the convolutional decoding is performed by applying the Viterbi algorithm on the received codeword and two types of decoding can be performed, the soft decision decoding (SDD) and the hard decision decoding (HDD). Now, because of data encoding, the average energy per bit at the output of the encoder is reduced by the coding rate R_c and given as $E_c = R_c E_b$, where E_b is the average energy per information bit at the input of the encoder. In this case, the average BER at the demodulator output, instead of (1), is given by

$$P_{eG}^{encoding} = Q\left(\sqrt{2\gamma_c}\right) \tag{7}$$

where $\gamma_c = \frac{E_c}{N_o}$ is the average SNR per bit in case of data encoding. The BER at the output of the decoder depends on the decoder type, either Hamming or convolutional, and on whether the decoder uses SDD or HDD. For Hamming codes, considering HDD, the BER at the decoder output can be approximated as [30]

$$P \approx P_{eG}^{encoding} - P_{eG}^{encoding}\left(1 - P_{eG}^{encoding}\right)^{n-1}. \tag{8}$$

For convolutional codes, the BER for HDD and SDD can be bounded, respectively, as [27, Eq. (8.2-32)] and [27, Eq. (8.2-26)]

$$\begin{aligned} P &\leq \sum_{d=d_{free}}^{\infty} B_d \left[2\sqrt{P_{eG}^{encoding}\left(1 - P_{eG}^{encoding}\right)}\right]^{d_{dfree}} \\ &\approx B_{d_{free}} \left[2\sqrt{P_{eG}^{encoding}\left(1 - P_{eG}^{encoding}\right)}\right]^{d_{free}} \end{aligned} \tag{9}$$

and

$$P \leq \sum_{d=d_{free}}^{\infty} B_d Q\left(\sqrt{2d\gamma_c}\right) \approx B_{d_{free}} Q\left(\sqrt{2d_{free}\gamma_c}\right) \tag{10}$$

where B_d's are the coefficients of the bit weight enumerating function (WEF) and d_{free} is the minimum Hamming distance of the code. For the encryption algorithm, under study in this paper, with data encoding, the BER at the output of the P/S convertor for the first encrypted block B_1 is given, in analogy to (2), as

$$P_{eE}^{encoding} = 0.5\left(1 - [1 - P]^{\beta_l}\right) \tag{11}$$

and for the remaining blocks, $B_2, B_3, \cdots, B_{N_b N_F}$, is given, in analogy to (4), as

$$P_{eXOR}^{encoding} = P + P_{eE}^{encoding} - 2PP_{eE}^{encoding} \tag{12}$$

where P is given by (8), (9) or (10). Now, we can write the superframe average BER, in analogy to (5), as

$$P_{e_{proposed}}^{encoding} = \frac{P_{eE}^{encoding} + \beta_c P_{eXOR}^{encoding}}{\beta_c + 1}. \tag{13}$$

Similar to (6), in the case of using heavy conventional encryption all over the whole blocks with data encoding, the superframe average BER in (13) reduces, as expected, to

$$\begin{aligned} P_{e_{conv}}^{encoding} &= \frac{P_{eE}^{encoding} + (N_b N_F - 1)P_{eE}^{encoding}}{N_b N_F} \\ &= P_{eE}^{encoding}. \end{aligned} \tag{14}$$

Now, instead of encoding all of the superframe blocks, we propose to encode only the first block, B_1, of each superframe, as it is the only block that will experience avalanche effect. In this case, the BER for B_1 at the output of the decryption stage is given by (11), while the BER for the remaining blocks, $B_2, B_3, \cdots, B_{N_b N_F}$, before the XORing is given by (1) and after the XORing is given by

$$P_{eXOR}^{first} = P_{eE}^{encoding} + P_{eG} - 2P_{eG}P_{eE}^{encoding} \tag{15}$$

and the overall superframe average BER is given by

$$P_{e_{proposed}}^{first} = \frac{P_{eE}^{encoding} + \beta_c P_{eXOR}^{first}}{\beta_c + 1}. \tag{16}$$

Similarly, for the case of using heavy conventional encryption all over the whole blocks while only the first block is encoded, the overall superframe average BER can be given as

$$\begin{aligned} P_{e_{conv}}^{first} &= \frac{P_{eE}^{encoding} + (N_b N_F - 1)P_{eE}}{N_b N_F} \\ &= \frac{P_{eE}^{encoding} + \beta_c P_{eE}}{\beta_c + 1}. \end{aligned} \tag{17}$$

where P_{eE} and $P_{eE}^{encoding}$ are given by (2) and (11), respectively.

Table 1 is the BER formulas comparisons table, which summarizes the ultimate equation numbers used to compute the BER performance of the conventional and the proposed encryption models for the three scenarios of no data encoding, data encoding, and first block data encoding.

IV. THROUGHPUT ANALYSIS OF LIGHTWEIGHT ENCRYPTION MODEL PROPOSED IN [25]

In this section, we provide throughput analysis for both the lightweight encryption algorithm proposed in [25] and the conventional encryption algorithms considering the two cases of with and without data encoding. In general, the throughput T can be defined as the number of correctly received information-carrying bits per second, which can be mathematically written in terms of the bit rate R as

$$T = R(1 - p_e)^{\beta_l} \tag{18}$$

where $(1 - p_e)^{\beta_l}$ is the probability of correct reception of β_l-bits length block with average BER of p_e. For a superframe with $N_F N_b$ blocks, the average throughput can be obtained by averaging the throughput amounts of all the blocks within the superframe, i.e.

$$T = \frac{1}{N_F N_b} \sum_{i=1}^{N_F N_b} R_i (1 - p_{e_i})^{\beta_l}. \tag{19}$$

TABLE 1. BER formulas comparisons table.

	Conventional Encryption Model	Lightweight Encryption Model Under Study
BER without data encoding	eq.(6) with eq.(2) and eq.(1)	eq.(5) with eq.(4), eq.(2), and eq.(1)
BER with data encoding	eq.(14) with eq.(11) and eq.(7)	eq.(13) with eq.(12), eq.(11), and eq.(7)
BER with first block encoded	eq.(17) with eq.(11) and eq.(2)	eq.(16) with eq.(15) and eq.(11)

TABLE 2. Throughput formulas comparisons table.

	Conventional Encryption Model	Lightweight Encryption Model Under Study
Without data encoding	$T_{conv} = \frac{\eta R(1-P_{eE})^{\beta_l} + \beta_c \eta R(1-P_{eE})^{\beta_l}}{\beta_c+1} = \eta R(1-P_{eE})^{\beta_l} \quad (20)$	$T_{proposed} = \frac{\eta R(1-P_{e_E})^{\beta_l} + \beta_c R(1-P_{e_{XOR}})^{\beta_l}}{\beta_c+1} \quad (21)$
With data encoding	$T^{encoding}_{con} = \frac{\eta R_c R(1-P^{encoding}_{e_E})^{\beta_l}}{\beta_c+1} + \frac{\beta_c \eta R_c R(1-P^{encoding}_{e_E})^{\beta_l}}{\beta_c+1} = \eta R_c R(1-P^{encoding}_{e_E})^{\beta_l} \quad (22)$	$T^{encoding}_{proposed} = \frac{\eta R_c R(1-P^{encoding}_{e_E})^{\beta_l}}{\beta_c+1} + \frac{\beta_c R_c R(1-P^{encoding}_{e_{XOR}})^{\beta_l}}{\beta_c+1} \quad (23)$
With first block encoded	$T^{first}_{con} = \frac{\eta R_c R(1-P^{encoding}_{e_E})^{\beta_l}}{\beta_c+1} + \frac{\beta_c \eta R(1-P_{e_E})^{\beta_l}}{\beta_c+1} \quad (24)$	$T^{first}_{proposed} = \frac{\eta R_c R(1-P^{encoding}_{e_E})^{\beta_l}}{\beta_c+1} + \frac{\beta_c R(1-P^{first}_{e_{XOR}})^{\beta_l}}{\beta_c+1} \quad (25)$

Because here we evaluate the superframe average throughput for information-carrying bits, the effective transmission data rate of the encrypted block is considered to be $R_{encry} = \eta R$, where $\eta < 1$ because of the overhead. In addition, the effective transmission data rate of the encoded block is considered to be $R_{encoding} = R_c R$, where $R_c < 1$ is the coding rate. By these considerations, we write the superframe average throughput for the lightweight encryption algorithm in [25] and for the conventional encryption algorithm considering the cases of (i) without data encoding, (ii) encoding all the blocks and (iv) encoding only the first block, respectively, as shown in Table 2.

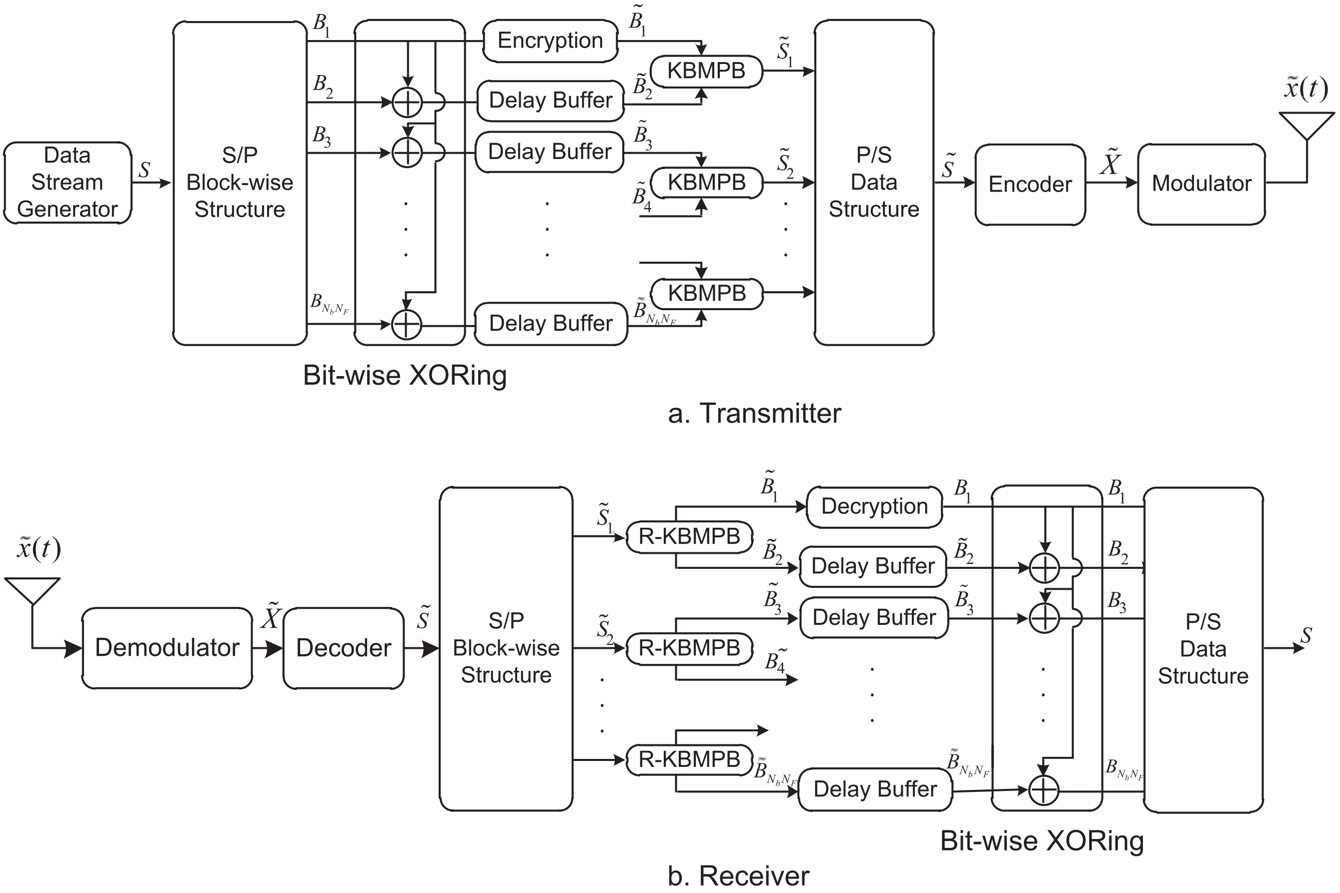
All of the BER and throughput expressions reported in this paper are obtained considering AWGN channels. To generalize these expressions for the case when the channel experiences fading in addition to noise, we average these results over the probability density function (PDF) of the instantaneous signal-to-noise ratio γ of the assumed fading model. For example, for a Rayleigh fading channel, we average the results over the PDF of the instantaneous SNR γ of the Rayleigh distribution, which is exponential with parameter $\bar{\gamma}_b$, as

$$\overline{P_e} = \int_0^\infty P_e(\gamma).\frac{1}{\bar{\gamma}_b}\exp(\frac{\gamma}{\bar{\gamma}_b})d\gamma \tag{26}$$

and

$$\overline{T} = \int_0^\infty T(\gamma).\frac{1}{\bar{\gamma}_b}\exp(\frac{\gamma}{\bar{\gamma}_b})d\gamma \tag{27}$$

After analyzing the error and throughput performance of the lightweight encryption model under study considering realistic scenarios, in the following section, we propose a new modification on its mechanism to further enhance its security level but without significantly affecting its heaviness as a lightweight encryption model.



a. Transmitter

b. Receiver

FIGURE 4. Transceiver Structure (Modified by adding KBMPB and R-KBMPB operations to enhance security of the proposed lightweight encryption mechanism in [25]).

V. ENHANCED LIGHTWEIGHT ENCRYPTION MODEL

A. PROPOSED SECURITY ENHANCEMENT

In order to enhance the security level of the lightweight encryption model under study, we propose adding a new security process box to be implemented after the bit-wise XORing process in Fig. 1.a, which we name as Key-Based Multiplexed Permutation Box (KBMPB). This process is reversed before the bit-wise XORing process in Fig. 1.b, which is equivalent to a process we name as Reverse Key-Based Multiplexed Permutation Box (R-KBMPB). Thus, the proposed new transceiver can be implemented as shown in Fig. 4. Again, the difference between this figure and Fig. 1 is the addition of the KBMPB and R-KBMPB blocks, as shown. The transmission algorithm of this proposed security-enhanced lightweight encryption model is detailed in the text structure in Algorithm 2. Notice that Algorithm 2 is an extended version of Algorithm 1 with improved security. The added new step in Algorithm 2 is the KBMPB operation.

The KBMPB box is applied at the output blocks $\tilde{B}_j$, in pairwise, as shown in Fig. 4a above. KBMPB is a new technique we propose to be used to enhance security without the need for implementing the strict avalanche criterion. The KBMPB operation has four inputs to it and one output. Two inputs are the blocks $\tilde{B}_j$ and $\tilde{B}_{j+1}$ as shown in Fig. 4a, and the other two inputs are secret keys each associated with each of these two input blocks $\tilde{B}_j$ and $\tilde{B}_{j+1}$. The function of the KBMPB is to multiplex the two input ciphertext blocks $\tilde{B}_j$ and $\tilde{B}_{j+1}$ into one double-sized block by scrambling using secret keys. The output block of the KBMPB, $\tilde{S}_m$ with $m = \{1, 2, \cdots, \frac{N_bN_F}{2}\}$, shown in Fig. 4a, is considered to be the final secure ciphertext that will be transmitted over the wireless communication channel, after coding and modulation.[3] It is obvious that this proposed modification with the added KBMPB process further enhances the security level of the lightweight encryption algorithm under study. This can be justified by the fact that even in the case that B_1 is detected by intruders, the other blocks $B_2, B_3, \cdot, B_{N_bN_F}$ will not be recovered as the secret keys of the KBMPB operation are supposed to be unknown. In addition, this attained security enhance-

[3] The idea of our proposed KBMPB process is inspired by the idea of Round 17 process proposed in [6] to improve the DES algorithm. However, in Round 17 in [6] an input block of size 64 bits is mapped into an output block of size 128 bits (see [6, Fig. 2]), i.e, there is a waste of half size in the output block which results in reducing data throughput by factor of two. On the other hand, in our proposed KBMPB (see Fig. 5) two input blocks each with size 128 bits are randomly multiplexed and mapped into one double-sized 256 bits output block, i.e., the overall data throughput is kept unchanged.

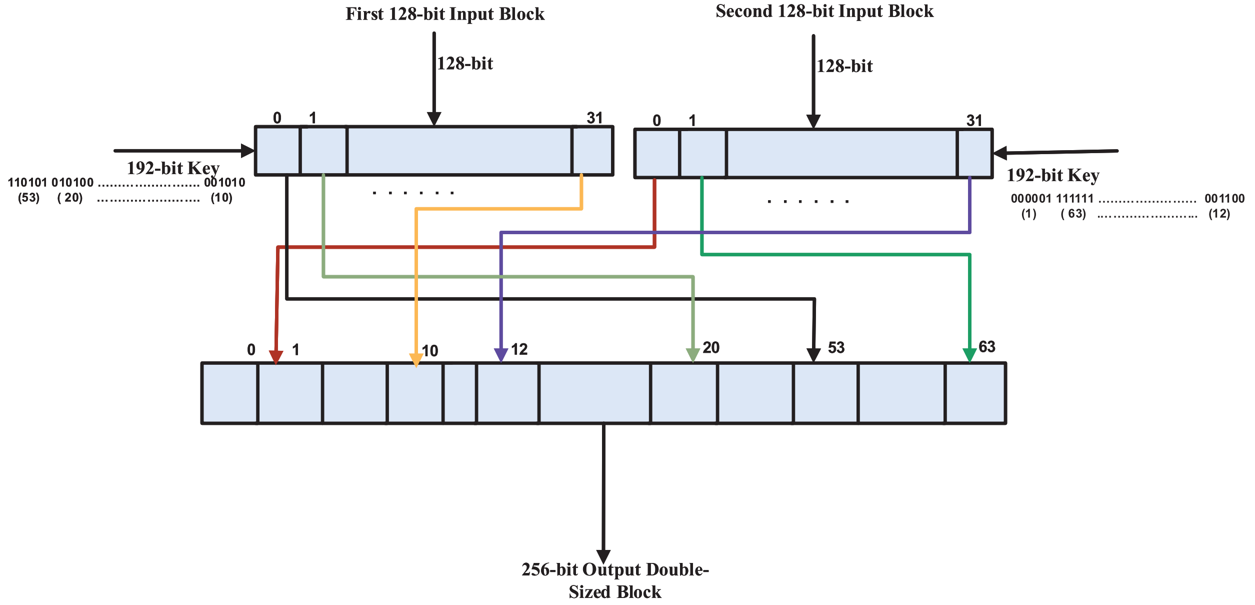


FIGURE 5. The mechanism of the KBMPB.

ment does not break the feature that the algorithm is still lightweight as the added overhead and processing time are related to the KBMPB and R-KBMPB mechanisms, which are light as compared to the heavy computational operations and rounds performed in classical encryption algorithms like the AES.

B. KBMPB MECHANISM

The mechanism of the KBMPB is described as follows. Each of the two input blocks to it is divided into sub-frames of 4 bits each. The length of the output block of the KBMPB is double-sized as compared to each of its ciphertext input blocks. Therefore, each of the first input block sub-frames is scrambled within distinct sub-frames in the output block with an appropriate associated secret key for all the sub-frames of the first block. The other input block sub-frames can be scrambled within the remaining empty sub-frames in the output block using a separate appropriate secret key for the whole sub-frames of the block. It should be noted here that the two scrambling secret keys should be selected in a way such that the sub-frames assigned in the output block to the first input block do not collide with the ones assigned to the second input block. In the proposed mechanism, each of the two inputs, to the KBMPB, is a 128-bit block size (i.e., $K = \beta_l = 128$). These two blocks are scrambled and multiplexed into a 256-bit cipher block size output using two distinct secret keys of 192-bit size each with a mapping procedure explained in Fig. 5. In this procedure, each of the 128-bit inputs is divided into 32 sub-frames of four bits each, which are mapped into an output cipher block of 64 sub-frames four bits each (256-bit block size). To achieve this mapping (64 sub-frames), each of the two inputs needs a secret key of size 192 bits (32 sub-keys of 6 bits each). For each (input, key) pair, each 6-bit sub-key of the 192-bit key is used to map one of the 4-bit input sub-frames of the 128-bit input block into one 4-bit output sub-frame of the 256-bit cipher block output. So, for each pair, the input sub-frames are scrambled randomly into 32 out of the 64 output sub-frames according to the associated key. The remaining 32 sub-frames of the output are randomly filled with the sub-frames of the other input block according to the other secret key. For the example shown in Fig. 5, suppose the first 6 bits of the key are 000101 (decimal 5). This means that the first 4-bit sub-frame of the input will be mapped into the fifth 4-bit sub-frame of the output. The secret keys are assumed to be known to the destination so it will be able to recover the individual 128-bit ciphertext blocks out of the total 256-bit received ciphertext using the R-KBMPB operation. To summarize, the proposed enhanced lightweight encryption has a plaintext of 128-bit size, an overall ciphertext of 256-bit size, and an overall key of 512-bit size (128 + 192+192).

C. PERFORMANCE OF ENHANCED-SECURITY ALGORITHM

Literally, adding the KBMPB and R-MBMPB operations in the enhanced-security lightweight encryption algorithm proposed above does not deteriorate the error rate and throughput performance as compared to that of the original algorithm before adding the KBMPB and R-MBMPB operations. This is due to the fact that, at the receiving side shown in Fig. 4b, re-scrambling the data bits back to their original positions using the R-KBMPB operation definitely does not affect the fact that they were detected correctly or erroneously. Therefore, all BER and throughput analytical expressions derived in Sections III and IV are also valid for this enhanced-security algorithm.

```
Input: Data stream as plaintext
Output: Data stream as ciphertext
Divide the data sequence into $N$ superframes;
foreach $N_i$ superframe $SF_i$, $i = 1, \ldots, N$, to be sent do
    Divide each superframe into $N_F$ frames;
    Divide the frame $(F_k)$, $k = 1, \ldots, N_F$, into $N_b$
    blocks with block size of $K = \beta_l$;
    Encrypt the first block $B_1$ with an appropriate
    encryption algorithm, i.e., $\tilde{B}_1 = E_k\,[B_1]$
    foreach of the remaining blocks $B_j$,
    $j \in \{2, 3, \ldots, N_bN_F\}$ do
        $\tilde{b}_{i,j} = b_{i,j} \oplus b_{i,1}$, $i \in \{0, 1, \ldots, K-1\}$;
        Generate the cipher blocks as
        $\tilde{B}_j = [\tilde{b}_{0,j}, \ldots, \tilde{b}_{K-1,j}]$ ;
    end
    foreach pair $\tilde{B}_{2m-1}, \tilde{B}_{2m}$, $m \in \{1, 2, \ldots, \frac{N_bN_F}{2}\}$ do
        $\tilde{S}_m = \text{KBMPB}[\tilde{B}_{2m-1}, \tilde{B}_{2m}]$; where KBMPB is
        the key-based multiplexed permutation operation
    end
    Generate the cipher frame as
    $\tilde{S} = [\tilde{S}_1, \tilde{S}_2, \cdots, \tilde{S}_{\frac{N_bN_F}{2}}]$;
end
Generate the cipher superframe accordingly. Repeat for
other superframes;
```

Algorithm 2 The Enhanced Lightweight Encryption

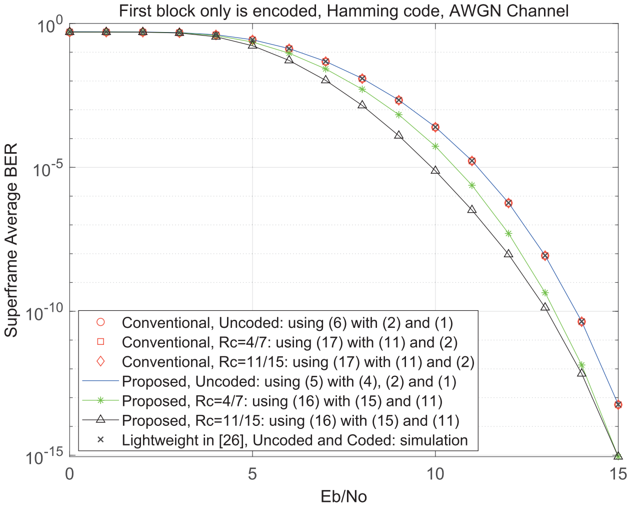


FIGURE 6. Superframe average BER performance for the lightweight encryption algorithm under study and that for the conventional AES and the lightweight proposed in [26] with Hamming code over AWGN channel. $N_f = 100$, $N_b = 10$, and $\beta_l = 128$.

VI. NUMERICAL RESULTS

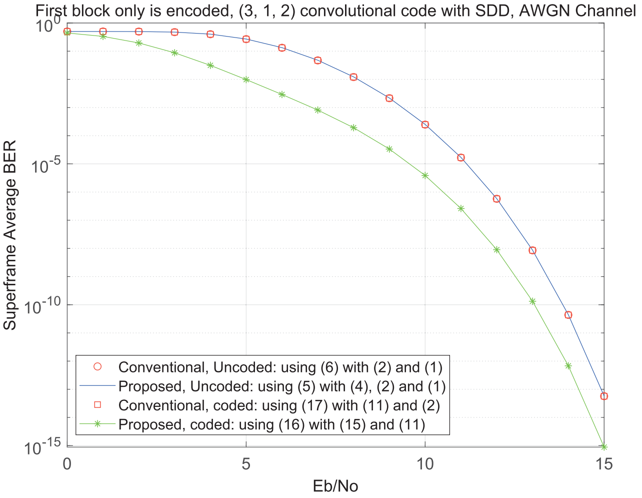


FIGURE 7. Superframe average BER performance for the lightweight encryption algorithm under study and that for the conventional AES with convolutional code over AWGN channel. $N_f = 100$, $N_b = 10$, and $\beta_l = 128$.

In this section, we provide numerical results to compare between the performance of lightweight encryption algorithm under study in one side and the conventional AES encryption algorithm and the image lightweight encryption algorithm proposed in [26] in the other side. This comparison is in terms of the superframe average BER and the normalized throughput. The results for our particular lightweight and the conventional encryption algorithms are obtained using the derived BER and throughput analytical expressions summarized in Table1 and Table 2, respectively. On the other hand, the results for the image lightweight encryption algorithm proposed in [26] are obtained through MATLAB simulation.[4] We consider AWGN channel that experiences Rayleigh fading, and two types of data encoders (to encode the first block of each superframe), LBC Hamming code and (3, 1, 2) convolutional code with transform domain generator matrix $G(D) = [1 + D, 1 + D^2, 1 + D + D^2]$, $B_{d_{free}} = 1$ and $d_{free} = 7$. We also assume the following parameters' values: $N_F = 100$, $N_b = 10$, $\beta_l = 128$, and $\eta = 0.8$.

In Fig. 6, we compare between the three considered encryption models in terms of the superframe average BER over the AWGN channel. First, we can observe from this figure that the lightweight image encryption algorithm proposed in [26] (with image size as the AES block size of 128 bits) offers same poor BER performance as that of the conventional AES for both cases with or without data channel-encoding. Because of that, in the following figures we restrict the comparison to be between the AES and our lightweight encryption algorithm. However, we can also observe from Fig. 6 that the our lightweight algorithm does not improve the BER performance when the data is not encoded by any error correction code. By having the first block not encoded, it results in avalanche in this block, after decryption. This error that occurs after decrypting the first block (avalanche)

[4] We have directly used the open source MATLAB code written by the authors of [26] to simulate the encryption/decryption processes of their proposed image lightweight encryption algorithm. Specifically, we have extended this MATLAB simulation code to be used to evaluate the error rate and throughput performance of the image encryption algorithm proposed in [26]. This extension has been done by adding the stages of the encoder, the modulator, the channel, the demodulator, the decoder, and the error rate counter.

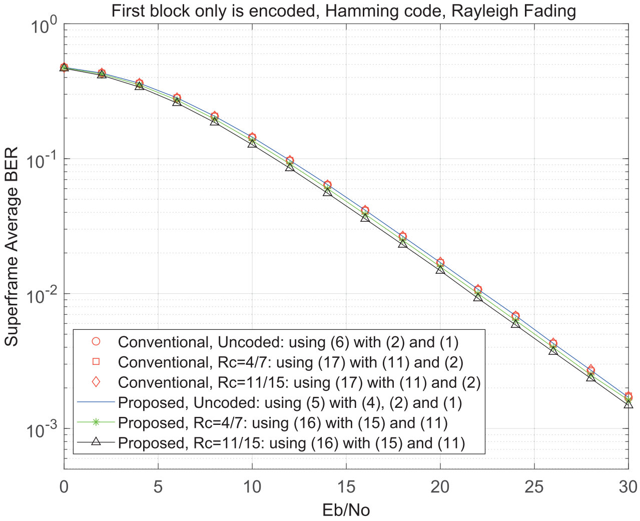


FIGURE 8. **Superframe average BER performance for the lightweight encryption algorithm under study and that for the conventional AES with Hamming code over Rayleigh fading channel. $N_F = 100$, $N_b = 10$, and $\beta_I = 128$.**

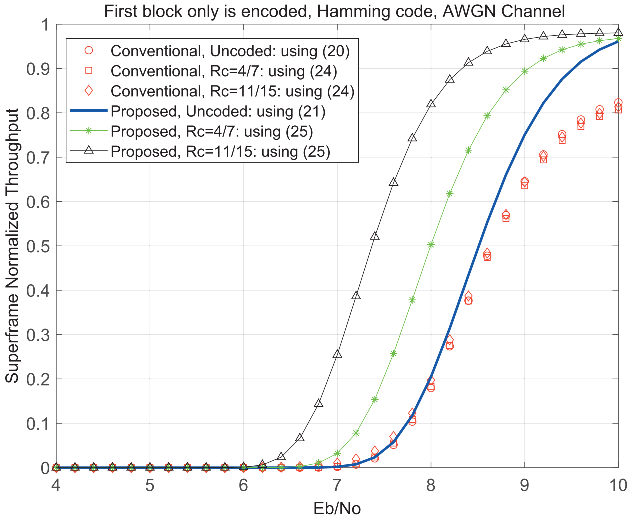


FIGURE 10. **Superframe average throughput performance for the lightweight encryption algorithm under study and that for the conventional AES with Hamming code AWGN channel. $N_F = 100$, $N_b = 10$, $\beta_I = 128$, and $\eta = 0.8$.**

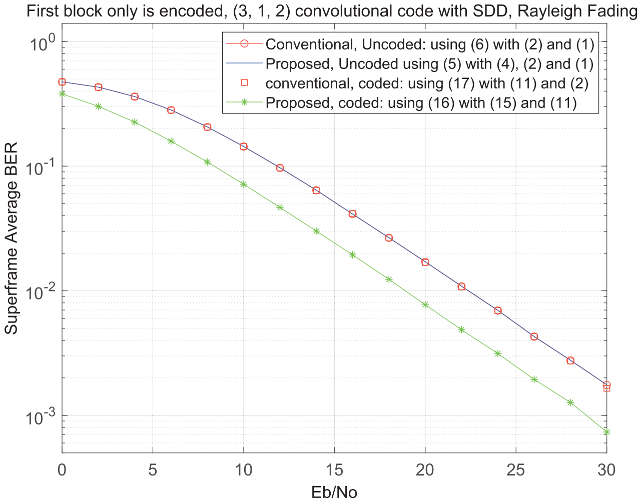


FIGURE 9. **Superframe average BER performance for the lightweight encryption algorithm under study and that for the conventional AES with convolutional code over Rayleigh fading channel. $N_F = 100$, $N_b = 10$, and $\beta_I = 128$.**

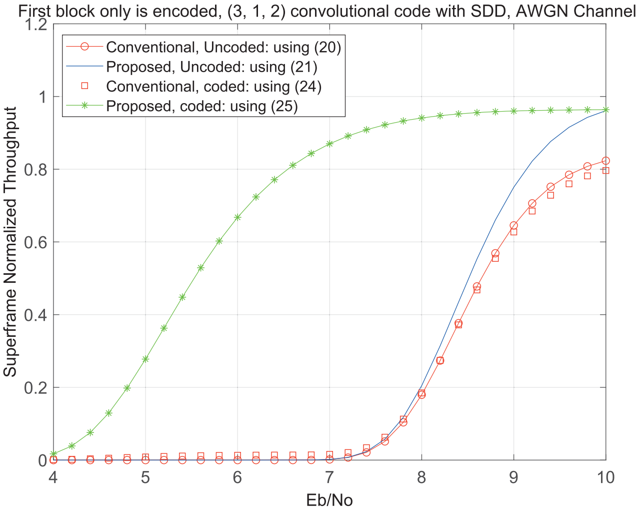


FIGURE 11. **Superframe average throughput performance for the lightweight encryption algorithm under study and that for the conventional AES with convolutional code over AWGN channel. $N_F = 100$, $N_b = 10$, $\beta_I = 128$, and $\eta = 0.8$.**

will propagate throughout the whole remaining blocks via the XORing operation at the receiver as shown in Fig. 1. On the other hand, by encoding the first block of both algorithms via the Hamming code, the BER performance of our particular algorithm is improved while it does not improve for the conventional algorithm. This is because that encoding the first block in the proposed algorithm improves the BER of that block and this improvement is reflected to the remaining blocks through the XORing at the receiver, keeping in mind that all these remaining blocks don't experience avalanche after decryption at the receiver. Whereas, in the conventional encryption case, all transmitted blocks will experience avalanche effect after decryption, at the receiver, and hence encoding only the first block improves its own BER while the remaining blocks will still experience avalanche effect. From Fig. 7 we can also notice that applying the convolutional code on the above scenario gives same observations. Furthermore, improvements achieved by our algorithm are also noticeable for the case of fading channels as well, see Fig. 8 and Fig. 9. From these two figures, we can also notice that, in case of fading channels, the improvement occurred by our algorithm is much better in the case of applying the convolutional code as compared to Hamming code. The reason for that is related to the code design where the convolutional code is more suitable than the Hamming code in fading channel environments.

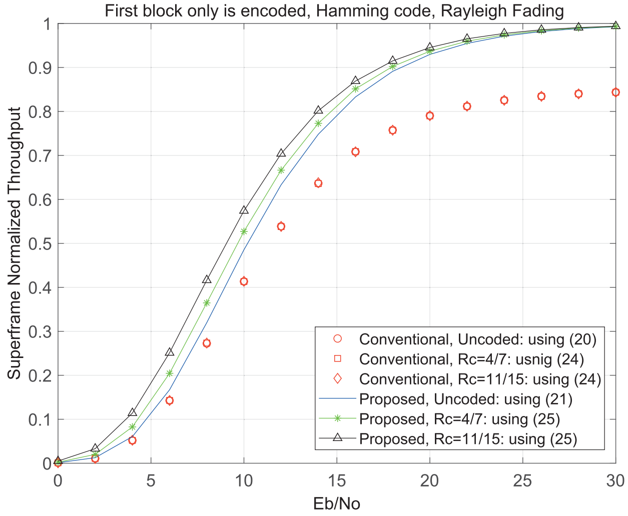


FIGURE 12. **Superframe average throughput performance for the lightweight encryption algorithm under study and that for the conventional AES with Hamming code over Rayleigh fading channel. $N_F = 100$, $N_b = 10$, $\beta_I = 128$, and $\eta = 0.8$.**

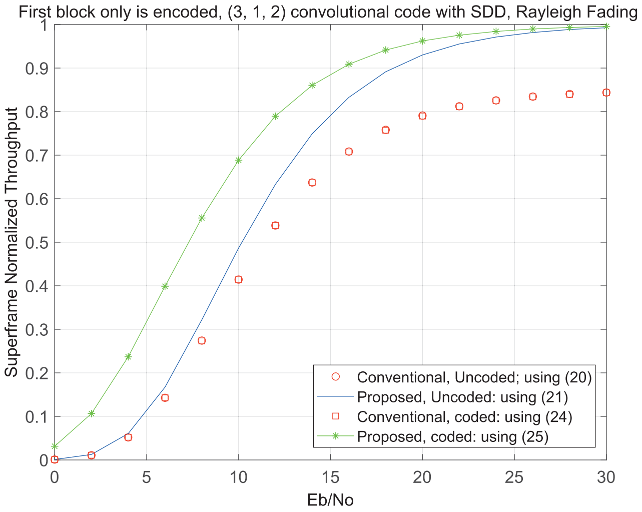


FIGURE 13. **Superframe average throughput performance for the lightweight encryption algorithm under study and that for the conventional AES with convolutional code over Rayleigh fading channel. $N_F = 100$, $N_b = 10$, $\beta_I = 128$, and $\eta = 0.8$.**

Fig. 10 and Fig. 11 compare between the superframe normalized throughput for our particular algorithm and the conventional one over the AWGN channel with Hamming and convolutional codes, respectively. It is obvious from these two figures that our lightweight algorithm provides higher throughput over the conventional algorithm regardless whether the data is encoded or not. Moreover, in case of data encoding, there is no noticeable improvement appears on the conventional algorithm throughput while improvement is obvious for the case of our algorithm. These observations are also valid for the case of fading channels, see Fig. 12 and Fig. 13.

VII. CONCLUSION

In this paper, we have revisited a lightweight encryption algorithm reported in literature and studied its performance in wireless channels in terms of bit error rate and data transmission throughput. In the lightweight encryption algorithm under study, using standard conventional heavy encryption such as AES is required only for one block among several blocks in a superframe, and hence large amounts of overhead and processing time delay reductions are achieved, which makes the algorithm most suitable for resource-limited devices used in IoT applications. The size of this block, which we referred to as the first block, is determined by the conventional encryption algorithm used for this first block. In this algorithm, all the remaining blocks of the information are then transmitted securely over the channel without a need for using heavy encryption. BER and throughput are vital performance metrics when it comes to interfacing Big Data with resource-limited devices especially in a wireless environment with severe fading and limited bandwidth. Therefore, we evaluated the performance of this proposed algorithm in terms of BER and throughput considering the AWGN channel that also experiences Rayleigh fading. To investigate the effects of the error correction codes on this performance evaluation, we have considered two types of data encoding; the Hamming code and the convolutional code, where we have only assumed encoding the first encrypted block, which also results in reduced overhead and computational complexity in addition to achieving higher data throughput as compared to conventional encryption schemes that assume applying heavy encryption (e.g., AES) to all the blocks in the superframe.

Furthermore, in this work, we have enhanced the security level of the lightweight encryption algorithm under study without significantly increasing its overhead size or computational complexity and also without affecting its error rate and throughput performance. Through numerical results, we have shown that the BER performance of the lightweight encryption algorithm under study is superior to that of the conventional encryption algorithms in the case when data encoding is implemented. In addition, the lightweight encryption algorithm under study has proven its throughput superiority over the conventional algorithm regardless whether the data is encoded or not as demonstrated by the numerical results reported in this paper. The mathematical framework presented in this paper is of its first kind in the field as applied to lightweight encryption and opens doors for evaluation other lightweight encryption algorithms proposed in literature for IoT and other emerging technology applications.

ACKNOWLEDGMENT

This manuscript has been co-authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

REFERENCES

[1] A. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1985, pp. 523–534.

[2] R. Forrié, "The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition," in *Proc. Conf. Theory Appl. Cryptogr.* New York, NY, USA: Springer, 1988, pp. 450–468.

[3] J. M. Reason, "End-to-end confidentiality for continuous-media applications in wireless systems," Ph.D. dissertation, Univ. California, Berkeley, Berkeley, CA, USA, 2001.

[4] W. Y. Zibideh and M. M. Matalgah, "The effect of the number of rounds and S-boxes on the error performance and security in a class of symmetric encryption algorithms," *Cyber J. Sel. Areas Telecommun.*, vol. 2, pp. 59–68, Jul. 2012.

[5] M. Haleem, C. Mathur, R. Chandramouli, and K. Subbalakshmi, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 4, pp. 313–324, Oct. 2007.

[6] W. Y. Zibideh and M. M. Matalgah, "Modified data encryption standard encryption algorithm with improved error performance and enhanced security in wireless fading channels," *Secur. Commun. Netw.*, vol. 8, no. 4, pp. 565–573, Mar. 2015.

[7] W. Y. Zibideh and M. M. Matalgah, "Computational complexity analysis for a class of symmetric cryptosystems using simple arithmetic operations and memory access time," *Int. J. Inf. Secur. Privacy*, vol. 7, no. 1, pp. 63–75, Jan./Mar. 2013.

[8] W. Y. Zibideh and M. M. Matalgah, "Key-based coded permutation ciphers with improved error performance and security in wireless channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 993–998.

[9] W. Y. Zibideh and M. M. Matalgah, "Energy consumptions analysis for a class of symmetric encryption algorithms," in *Proc. IEEE Radio Wireless Symp. (RWS), IEEE Radio Wireless Week (RWW)*, Newport Beach, CA, USA, Jan. 2014, pp. 268–270.

[10] W. Y. Zibideh and M. M. Matalgah, "A comprehensive platform-independent computational complexity analysis for a class of symmetric cryptosystems," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)-Commun. Inf. Secur. Symp.*, San Diego, CA, USA, Jan. 2013, pp. 374–379.

[11] W. Y. Zibideh and M. M. Matalgah, "An optimized encryption framework based on the modified-DES algorithm: A trade-off between security and throughput in wireless channels," in *Proc. IEEE Radio Wireless Symp. (RWS) Radio Wireless Week (RWW)*, Santa Clara, CA, USA, Jan. 2012, pp. 419–422.

[12] M. M. Matalgah, W. Z. Zibideh, and A. M. Magableh, "Alleviating the effect of the strict avalanche criterion (SAC) of symmetric-key encryption in wireless communication channels," in *Proc. Int. Conf. Commun. Inf. Technol. (ICCIT)*, Aqaba, Jordan, Mar. 2011, pp. 138–141.

[13] W. Y. Zibideh and M. M. Matalgah, "Modified-DES encryption algorithm with improved BER performance in wireless communication," in *Proc. IEEE Radio Wireless Symp. (RWS) Radio Wireless Week (RWW)*, Phoenix, AZ, USA, Jan. 2011, pp. 219–222.

[14] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan. 2015.

[15] S. Roy, U. Rawat, and J. Karjee, "A lightweight cellular automata based encryption technique for IoT applications," *IEEE Access*, vol. 7, pp. 39782–39793, 2019.

[16] S.-Y. Tan, K.-W. Yeow, and S. O. Hwang, "Enhancement of a lightweight attribute-based encryption scheme for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6384–6395, Aug. 2019.

[17] F. Hazzaa, S. Yousef, E. Sanchez, and M. Cirstea, "Lightweight and low-energy encryption scheme for voice over wireless devices," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2018, pp. 2992–2997.

[18] M. A. Habib, M. Ahmad, S. Jabbar, S. H. Ahmed, and J. J. Rodrigues, "Speeding Up the Internet of Things: LEAIoT: A lightweight encryption algorithm toward low-latency communication for the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 7, no. 6, pp. 31–37, Nov. 2018.

[19] X. Zhang, S.-H. Seo, and C. Wang, "A lightweight encryption method for privacy protection in surveillance videos," *IEEE Access*, vol. 6, pp. 18074–18087, 2018.

[20] S. Perez, J. L. Hernandez-Ramos, S. N. Matheu-Garcia, D. Rotondi, A. F. Skarmeta, L. Straniero, and D. Pedone, "A lightweight and flexible encryption scheme to protect sensitive data in smart building scenarios," *IEEE Access*, vol. 6, pp. 11738–11750, 2018.

[21] V. Dahiphale, G. Bansod, and J. Patil, "ANU-II: A fast and efficient lightweight encryption design for security in IoT," in *Proc. Int. Conf. Big Data, IoT Data Sci. (BID)*, Dec. 2017, pp. 130–137.

[22] A. Alabdulatif, H. Kumarage, I. Khalil, M. Atiquzzaman, and X. Yi, "Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure," *IET Wireless Sensor Syst.*, vol. 7, no. 6, pp. 182–190, Dec. 2017.

[23] A. Z. Alshamsi and E. S. Barka, "Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks," in *Proc. Int. Conf. Inform., Health Technol. (ICIHT)*, Feb. 2017, pp. 1–7.

[24] S. Koteshwara and A. Das, "Comparative study of authenticated encryption targeting lightweight IoT applications," *IEEE Design Test*, vol. 34, no. 4, pp. 26–33, Aug. 2017.

[25] M. M. Matalgah and A. M. Magableh, "Simple encryption algorithm with improved performance in wireless communications," in *Proc. IEEE Radio Wireless Symp.*, Jan. 2011, pp. 215–218.

[26] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT: A lightweight encryption algorithm for secure Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, pp. 402–411, 2017.

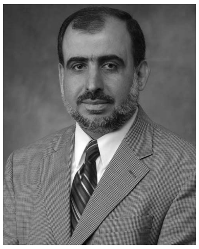
[27] J. G. Proakis, *Digital Communications*. New York, NY, USA: McGraw-Hill, 2014.

[28] M. M. Matalgah, "Error performance of cryptography transmission in wireless fading channels," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2019, pp. 1–4.

[29] S. Lin and D. J. Costello, *Error Control Coding*. London, U.K.: Pearson, 2001.

[30] B. Sklar and F. J. Harris, *Digital Communications: Fundamentals and Applications*, vol 2001. Englewood Cliffs, NJ, USA: Prentice-Hall, 1988.

YAZID M. KHATTABI (Member, IEEE) received the bachelor's degree in electrical engineering with a specialization in electronics and communications and the master's degree in electrical engineering with a specialization in wireless communications from the Jordan University of Science and Technology, Irbid, Jordan, in 2008 and 2010, respectively, and the Ph.D. degree in electrical engineering with a specialization in wireless communications from the Center for Wireless Communications (CWC), University of Mississippi, Oxford, MS, USA, in 2016. From March 2011 to December 2012, he served as a Telecommunications and Electronics Design Engineer with King Abdullah II Design and Development Bureau (KADDB), Amman, Jordan, with responsibilities included and not limited to telecommunication systems design for unmanned vehicles; electronics and RF printed circuits software design, implementation, and maintenance; RF planning and optimization; and signal propagation modeling. From 2013 to 2016, he served as a Research Assistant with CWC, University of Mississippi, where he received several research awards. Since August 2016, he has been with The University of Jordan, Amman, where he is currently an Assistant Professor of electrical engineering. His current research interests include several areas in wireless communications with emphasis on performance evaluation and optimization of cooperative and relaying systems, spatial modulation MIMO systems, powered systems, high-speed railway transportation systems, and encryption algorithms over fading channels. He is also serving as a reviewer for several refereed international journals and conferences.



MUSTAFA M. MATALGAH (Senior Member, IEEE) received the bachelor's and master's degrees in electrical engineering from Jordan and the Ph.D. degree from the University of Missouri, Columbia, USA. He has a wide range of academic and industry experiences in the electrical engineering field with emphasis on communication engineering. From 1996 to 2002, he was with Sprint, Kansas City, MO, USA, where he held various technical positions leading a wide range of projects dealing with optical communication systems deployment and the evaluation and assessment of wireless communication emerging technologies. Since August 2002, he has been with The University of Mississippi, Oxford, MS, USA, where he is currently a Full Professor of electrical engineering. In summer 2008, he was a Visiting Professor with Chonbuk National University, South Korea. He was also a Visiting Professor and program evaluator with Misr International University (MIU), Egypt, in summers of 2009, 2010, and 2012. He also held academic positions in Saudi Arabia and short-term positions in Jordan. He served on the Faculty Senate of The University of Mississippi for four years. His current technical and research experience is in the performance evaluation and optimization of wireless communication systems in fading channels. He has more than 150 archival publications (including journals, conference proceedings, book chapters, and patents) in addition to more than two dozens of industry technical reports in these areas. He served as the Research Supervisor of, and served on defense committees on, several M.Sc. and Ph.D. students. He received several certificates of recognition for his work accomplishments in the industry and academia. He was a recipient/co-recipient of the Best Paper Award on several international and regional conferences and workshops and a recipient of the 2006 School of Engineering Junior Faculty Research Award at The University of Mississippi. He is on Editorial Board of four International journals, served as a member and the Chair on several university committees, the Chair on several international conferences sessions and workshops, a member on several international conferences, technical program, and organizing committees, a reviewer for several funding proposals in USA and Canada, and a Project Manager on several projects in industry.

MOHAMMED M. OLAMA (Senior Member, IEEE) received the B.S. and M.S. (Hons.) degrees in electrical engineering from the University of Jordan, in 1998 and 2001, respectively, and the Ph.D. degree from the Electrical Engineering and Computer Science Department, The University of Tennessee, Knoxville, TN, USA, in 2007. From 1999 to 2001, he served as a full-time Control Engineer with National Electric Power Company, Amman, Jordan. He is currently a Research Scientist with the Computational Sciences and Engineering Division, Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, USA. He has been with ORNL, since 2007. He is also an Adjunct Associate Professor with the Electrical Engineering and Computer Science Department, The University of Tennessee. He has over 100 technical publications, including articles in refereed journals, conference proceedings, book chapters, and technical reports; and numerous presentations at professional conferences and international symposia. His research interests include smart grid and smart buildings; smart grid communications and control; building-to-grid integration; cyber-physical systems; complex systems; infrastructure modeling and analysis; wireless communications; 5G wireless networks; stochastic channel modeling, power control, and localization in wireless networks; wireless sensor networks; wireless security; big data integration and analytics; healthcare data analytics and hazard detection; statistical learning, forecasting, and inference algorithms; machine learning; artificial intelligence; statistical signal processing; and discrete-event simulation. He is a member of the Phi Kappa Phi Honor Society. He received the Best Paper Awards in the IEEE International Symposium on Power Electronics for Distributed Generation Systems, in 2018, and the Mediterranean Conference on Intelligent Systems and Automation, in 2008. He was a recipient of the Significant Event Award at ORNL, in 2007, and the Best Mentor Award at ORNL, in 2019.