The Effect of the Number of Rounds and S-Boxes on the Error Performance and Security in a Class of Symmetric Encryption Algorithms

Walid Y. Zibideh and Mustafa M. Matalgah

***Abstract*—The number of rounds and S-Boxes in any symmetric cryptosystem plays a great role on its security as well as on the probability of correct reception at the receiver after decryption. This work considers a class of symmetric encryption algorithms based on the data encryption standard (DES) and sheds lights into understanding the effect of each the number of rounds and number of S-Boxes on the security of the encrypted data as well as on the probability of correct reception in the wireless channel. In wireless channels, some encrypted bits could be flipped while transmitted over the channel due to noise, interference or fading. This degradation in the wireless channel conditions causes the data after decryption to have some amount of error that depends on the number of bits in error received in the encrypted data, before decryption, and on the location of these bits in the cipher block. We consider the number of rounds, the number of S-Boxes and the channel conditions (in terms of signal-to-noise power ratio (SNR)); and study their effect on security level and detection error performance. Using numerical computations and computer simulations, when considering a certain encryption mechanism, we present qualitative and quantitative analysis on the tradeoff between communication reliability and security levels versus the fluctuations in the wireless channel conditions.**

***Index Terms*—Encryption, S-Box, wireless channel, DES, M-DES.**

I. Introduction

Due to the fact that data transmitted over the wireless channel may experience noise, fading and interference, the encrypted data may be received in some amount of error. Due to the strict avalanche criterion (SAC) effect which was originally implemented in well-known encryption algorithms to ensure security, half the data of one block after decryption will be in error given that the block is received with even a single bit in error before decryption. Therefore, when the wireless channel experiences conditions such that one bit of the encrypted block is flipped, we say half the data of one block after decryption will be in error (avalanche effect). In conventional symmetric encryption and to achieve SAC, the encryption algorithm was designed carefully with appropriate numbers of S-Boxes and rounds implemented in the algorithm. In [1]-[4], the authors studied the effect of the S-Boxes and their design on the SAC. In [5], the authors proposed a new encryption algorithm that is a modification to the data encryption standard (DES) algorithm to alleviate the negative impact of SAC on communication integrity without tolerating the security level. To close the loop in [1]-[4] and to extend the work in [5], we take into account the number of rounds, the number of S-Boxes and the wireless channel condition as well to study their effect on security and error performance. In our evaluation, we consider the DES and a modified version of it, M-DES [5], as case studies. In the proposed algorithm in [5], the authors considered DES and dropped the number of S-Boxes from eight to two in order to alleviate SAC. Due to this reduction in the number of S-Boxes, the security of the encrypted data was significantly degraded. To overcome with this degradation, the authors introduced a new round which they called round 17. This round takes the 64-bit output of round 16 of DES and produces a 128-bit ciphertext using a new key of 80 bits. The proposed algorithm significantly improves the error performance compared to the traditional DES. In addition, by introducing the new round, the security is remarkably improved, such that a differential cryptanalysis is almost impossible. In this paper we extend the work in [5] by evaluating the security enchantment of the new round proposed therein in a more comprehensive way, where we numerically evaluate the probability of a successful attack on the proposed algorithm as well as calculating the time required for such an attack. In addition, we also evaluate the effect of number of rounds and number of S-Boxes on the probability of correct reception assuming different channel conditions (i.e. different signal-to-noise ratio (SNR) values). Moreover, we evaluate the effect of number of rounds and number of S-Boxes on the security level of the encrypted data in DES as well as in the new round proposed in [5]. The rest of the paper is organized as follows. In the next section we introduce a brief description of the data encryption standard (DES) and M-DES. The effect of the number of rounds and S-Boxes on the

Manuscript received July 10, 2012. Walid Zibideh is with Qualcomm Inc. San Diego, CA, 92122 USA (phone: 662-401-9886; e-mail: walidz@qualcomm.com).

Mustafa Matalgah is with the Electrical Engineering Department, University of Mississippi, Univeristy, MS 38677 USA, (e-mail: mustafa@olemiss.edu).

error performance is evaluated in section III with discussions. The effect of the number of rounds and S-Boxes on the security is analyzed in section IV with discussions. Finally, some conclusions are drawn in section V.

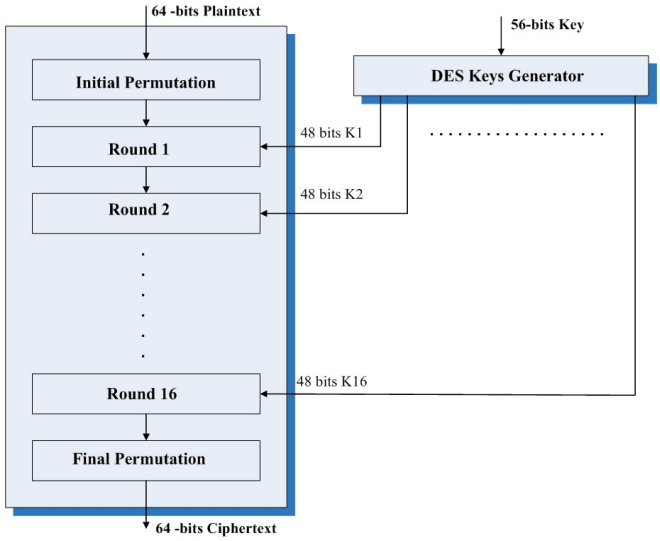


Fig. 1. DES Encryption Algorithm General Block Design

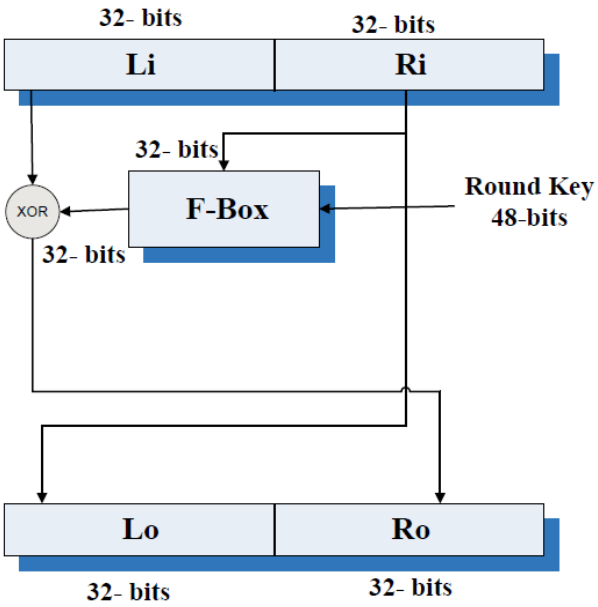


Fig. 2. DES Round Structure General Block Design

II. The Data Encryption Standard and M-DES

A. *DES*

The Data Encryption Standard (DES) is a symmetric "private" key block cipher. It was selected by the National Institute of Standards and Technology (NIST) to be used in encrypting all governmental documents in 1977. It was standardized as an official Federal information standard (FIPS 46). DES was designed by IBM and the National Security Agency (NSA), and was considered secure until 1999 when it was broken in 22 hours and 15 minutes due to its small size key [6], [7], [8]. The algorithm was originally designed with a 64-bit input (Plaintext) and a 64-bit output (ciphertext) with a 56-bit key, and consisted of sixteen identical rounds. Figure 1 shows the general architecture of DES. DES encryption consists of the following phases:

1. Initial Permutation
2. Rounds 1 through 16
3. Final Permutation

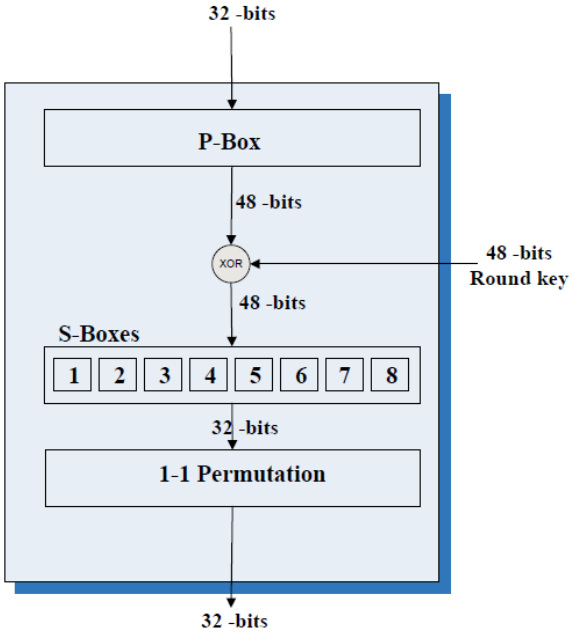


Fig. 3. F-Box Structure

Each round requires a different 48-bit key that is generated by the round key generator, which takes the 56-bit key as its input. In the following, we discuss each phase in details.

The initial and final permutation phases take a block input of 64 bits and generate an output block of the same size. The permutation is a process of changing the locations of the bits without changing the values of the bits, which is 1-1 bit mapping based on a fixed permutation table. The initial permutation is followed by 16 identical rounds where each round takes a block input of 64 bits that is cascaded from the output of the previous round. Here, the input of the first round is the output of the initial permutation phase, while the output of round 16 is the input for the final permutation phase. A block diagram of the DES round structure is shown in Figure 2. As shown in the figure, at the beginning of each round the 64-bit block is divided into two parts, left and right of 32 bits each. The right part is taken exactly as the left 32-bit output of the same round, while the left part is XOR-ed with the 32-bit output of the F-Box. The F-Box takes the right 32 bits input of the round and the 48-bit round key as its inputs. The F-Box is a function of the 48-bit round key and the right 32-bit half of the round inputs R_i, K_i. A block diagram of the F-Box structure is shown in Figure 3. As shown in the figure the round key is XOR-ed with the output of the expansion box (P-Box), which has the right 32 bits round input as its input and expands it to 48 bits output. The 48-bit result of the XOR

operation is the input for the S-Box. The 32-bit output of the S-Box phase is then permutated through 1-1 mapping (the same way as the initial and final permutation phases but with a new permutation table).

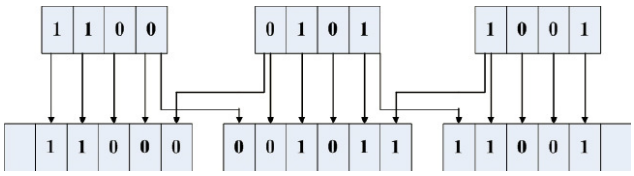
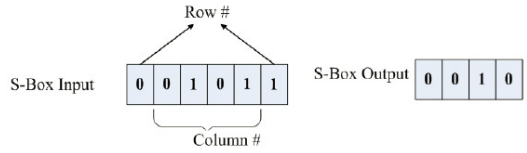


Fig. 4. P-Box mapping

1) P-Box

The expansion box is a 32-48 permutation box, in which 1 bit is mapped to one or two bits. The 32-bit input of the P-Box is mapped to a 48-bit output. The 32-bit input frame is divided into eight sub-frames each of four bits, and each sub-frame is mapped into a new sub-frame of six bits, which makes the output frame equal to 48 bits. The P-Box mapping is shown in Figure 4, where the four bits of the input sub-frame are mapped into the four middle bits of the output sub-frame, while the last bit of the previous input sub-frame is mapped to the first bit of the current output sub-frame, and the first bit of the next sub-frame is mapped to the last bit of the current output sub-frame.



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
01	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
10	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
11	15	12	8	02	04	09	01	07	05	11	03	14	10	00	06	13

Fig. 5. S-Box 1 mapping table

2) S-Box

The S-Box phase is the most responsible part for the bit mixing in DES. The 48-bit input frame of the S-Box phase is divided into eight sub-frames each of six bits. Each of the sub-frames is an input to one of the eight S-Boxes. Each S-Box takes an input of six bits and generates an output of four bits, and uses a 4×16 table for the mapping. The four middle bits of the six input bits are used as an index for the column in the mapping table and the two bits on the edges are used as an index for the row. Therefore, when any S-Box has an input, the input is mapped to an entry in the table and the value in the table is the output of the S-Box. An example for one of the eight S-Box mappings is shown in Figure 5. In the figure, the input for S-Box number one is 001011. The middle bits are 0101, which refers to the fifth column, while the edge bits are 01 which refers to the second row. So, the output is the entry at the intersection of the fifth column with the second row as shown in the figure.

B. M-DES

M-DES was introduced as a modification to the data encryption standard [5], by which the error performance is improved and the security is enhanced compared to DES. In general, the design of M-DES is very similar to the design of the data encryption standard, except in the S-Box and by introducing a new round called Round 17, which has its own key that is different from the original DES 56-bit key. M-DES has two main modifications to the standard DES. The first modification is that the number of distinct mapping tables is reduced from eight to two mapping tables. The second modification is the addition of a new round with a new 80-bit key to the original 16 rounds. Moreover, The S-Boxes were redesigned to reduce the error in M-DES, the first four S-Boxes uses similar mapping tables which are the same as the first mapping table of the standard DES, while the fifth through the eighth S-Boxes use similar mapping tables that are the same as the fourth S-Box mapping table in the standard DES.

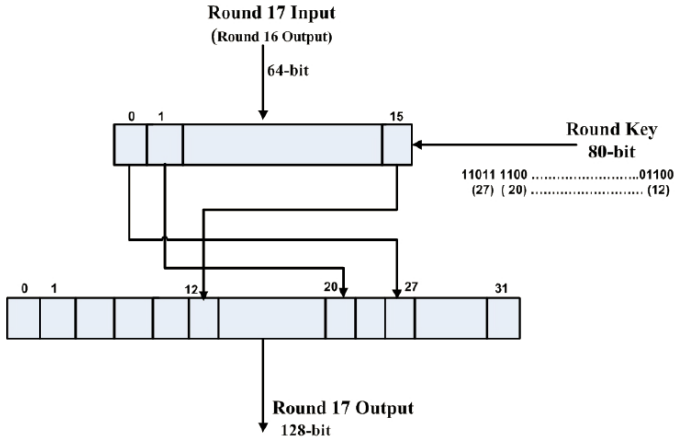


Fig. 6. Round 17 Design, mapping the 16 input sub-frames into the 32 output sub-frames using the 80-bit key

The reduction in the number of distinct mapping tables as well as the change in the design of the remaining mapping tables had significantly improved the error performance. On the other hand, this reduction and redesign in the S-Boxes mapping tables had reduced the security of the algorithm. To overcome this security reduction, a new round is introduced in M-DES by which the algorithm becomes in fact secure to both brute force and differential cryptanalysis attacks as will be shown later in the paper. Round 17 have two inputs and one output, the two inputs are the 64-bit output of the final permutation stage and an 80-bit key; the output is the 128-bit cipher. The 80-bit key is used to map the 64-bit input of Round 17 to a 128-bit output. This mapping procedure is shown in Figure 6 where the 64-bit input of round 17 is divided into sixteen sub-frames of four bits each and the 80-bit key is divided into 16 sub-keys, each of five bits, while the 128-bit output consists of 32 sub-frames of four bits each. Each five bits of the 80-bit key is used to map one of the 4-

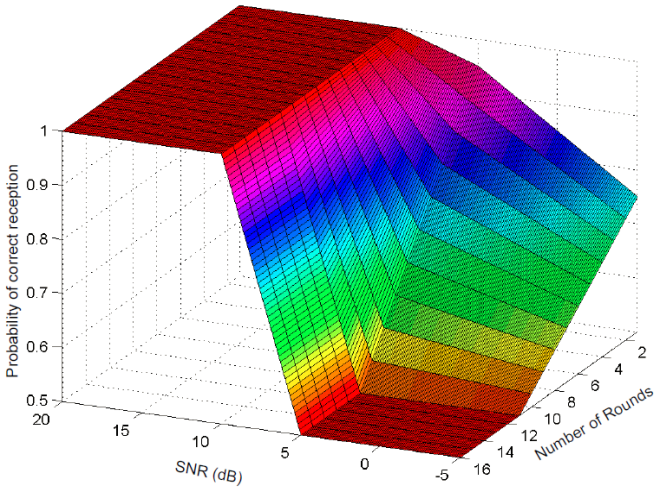


Fig. 7. The effect of the number of rounds and SNR on the probability of correct reception for a fixed number of distinct S-Boxes equal to eight

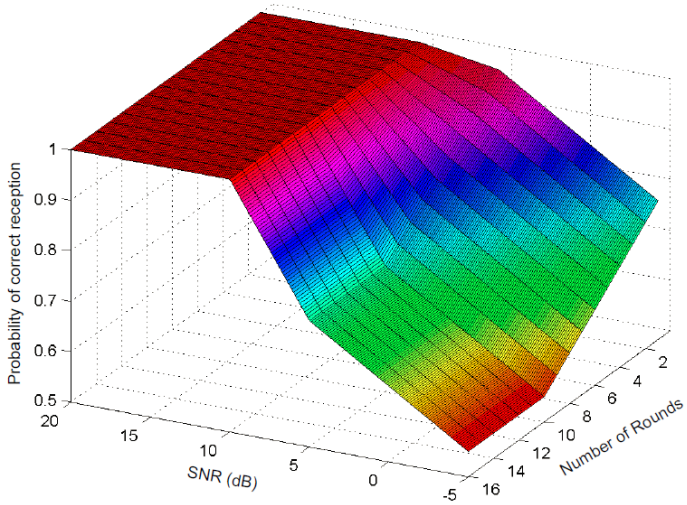


Fig. 8. The effect of the number of rounds and SNR on the probability of correct reception for a fixed number of distinct S-Boxes equal to four

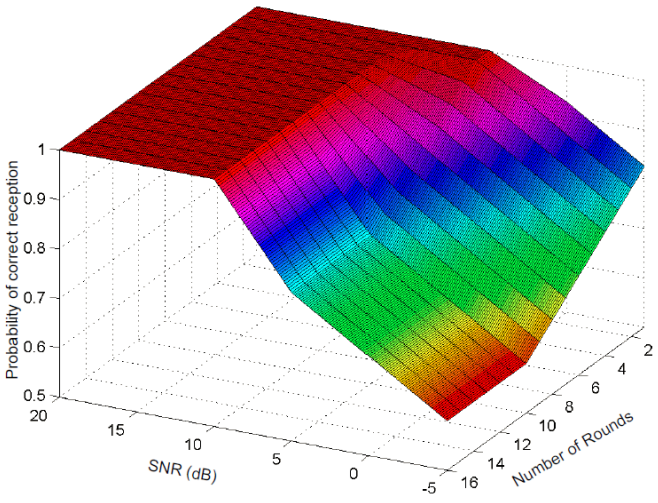


Fig. 9. The effect of the number of rounds and SNR on the probability of correct reception for a fixed number of distinct S-Boxes equal to two

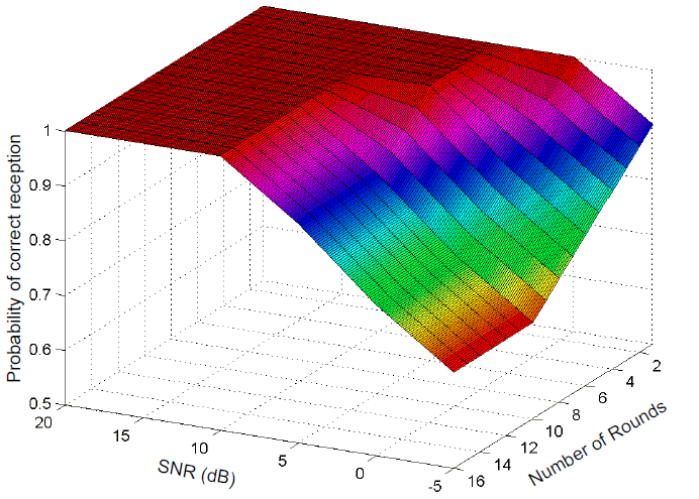


Fig. 10. The effect of the number of rounds and SNR on the probability of correct reception for a fixed number of distinct S-Boxes equal to one

bit input sub-frames to one 4-bit output sub-frame. So the input sub-frames will be scrambled randomly in 16 out of the 32 output sub-frames according to the key. The remaining 16 sub-frames of the output are randomly filled with zeros and ones. For example, suppose the first 5 bits of the key are \$00101\$. This illustrates that the first 4-bit sub-frame of the input will be mapped to the fifth 4-bit sub-frame of the output. The receiver is assumed to have the 80-bit key, so it will be able to recover the useful 64-bit ciphertext out of the total 128-bit received ciphertext. In summary, the proposed algorithm has a plaintext of 64 bits, an overall ciphertext of 128 bits, and an overall key of 136 bits. In the following section, we show the effect of number of rounds and S-Boxes on the probability of correct reception in both DES and M-DES.

III. Effect of the Number of Rounds and S-Boxes on the Error Performance

In this section we evaluate the effect of number of rounds and S-Boxes in different channel conditions (i.e., different SNR values) on the probability of correct reception for both DES and M-DES.

A. *Error Performance of DES*

Given that the probability of correct reception is evaluated based on three different factors (i.e., number of rounds, number of S-Boxes and the SNR), we assume three different scenarios in our analysis:

1. Fixing the number of S-Boxes and changing the number of rounds and the SNR
2. Fixing the SNR and changing the number of S-Boxes and the number of rounds
3. Fixing the number of rounds and changing the number of S-Boxes and the SNR

Figures 7-10 show different simulation results for the first scenario where the number of S-Boxes is fixed to eight, four, two and one in Figures 7, 8, 9 and 10, respectively. It can be noticed from Figure 7, where the number of S-Boxes is eight,

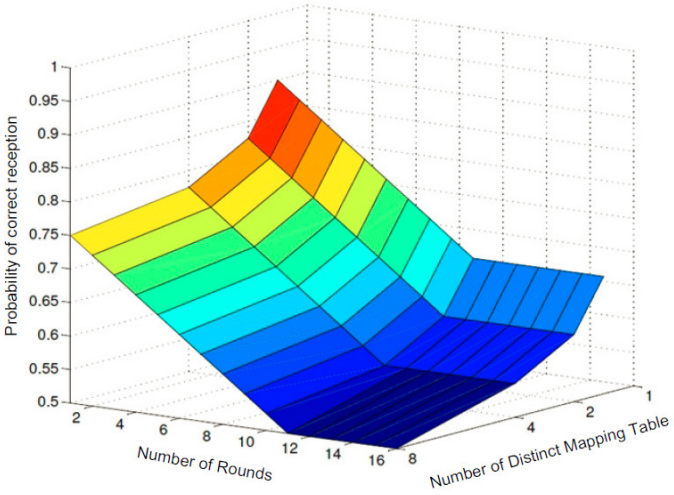


Fig. 11. The effect of the number rounds and the number of distinct number of S-Box mapping tables on the probability of correct reception for a fixed SNR equal to -5 dB

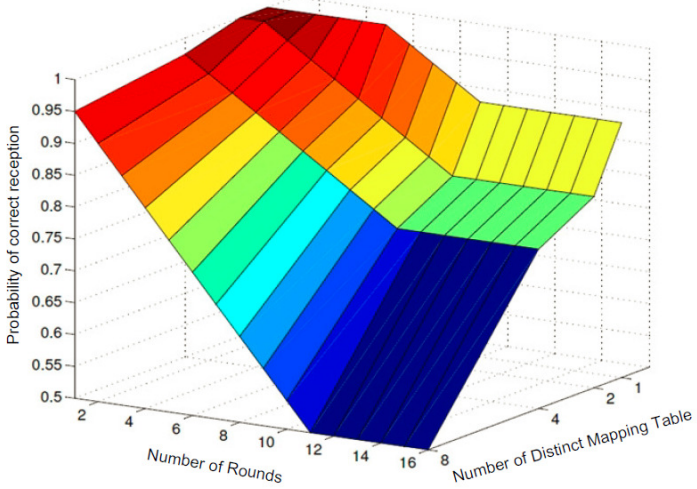


Fig. 13. The effect of the number rounds and the number of distinct number of S-Box mapping tables on the probability of correct reception for a fixed SNR equal to 5 dB

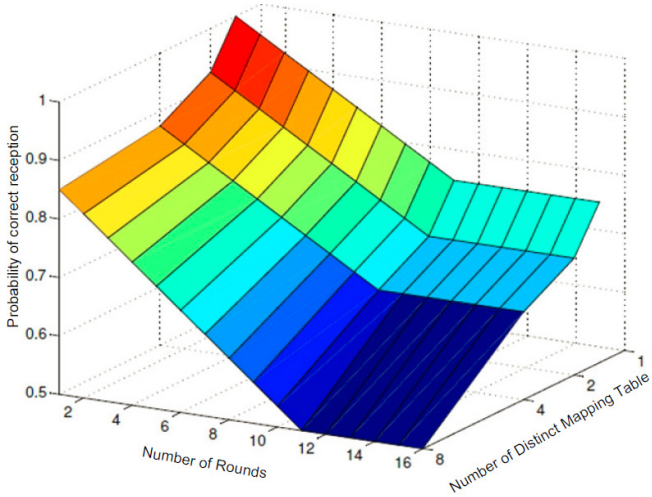


Fig. 12. The effect of the number rounds and the number of distinct number of S-Box mapping tables on the probability of correct reception for a fixed SNR equal to 0 dB

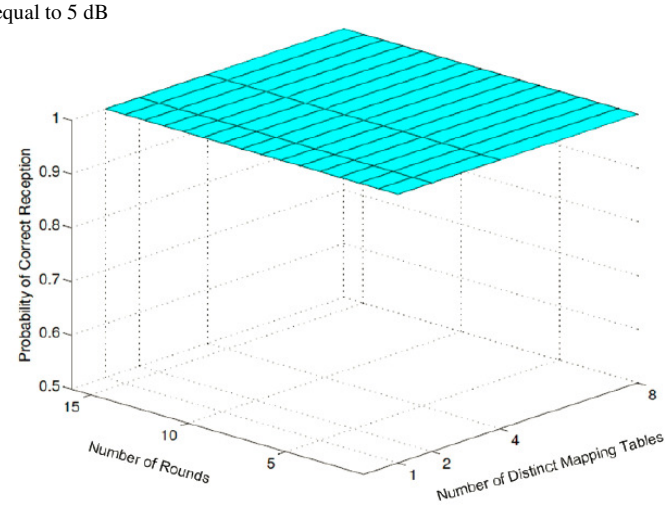


Fig. 14. The effect of the number rounds and the number of distinct number of S-Box mapping tables on the probability of correct reception for a fixed SNR equal to 10 dB

the number of rounds is changed from 1 to 16 and the SNR is changed from -5 to 20 dB, that the area bordered by SNR values from -5 to 5 dB and 16 to 12 rounds represents the Strict avalanche effect (SAC) area, because the probability of correct reception within this area is equal to 0.5. However, if we move to an area outside this range for example 8 rounds with an SNR equal to 0 dB, the probability of correct reception increases to 0.57. In general, we can conclude that when the number of rounds decreases, the probability of correct reception increases and when the SNR value increases the probability of correct reception will increase as well, as expected. The effect of these changes on the security of the encrypted data will be analyzed in the next section. Figures 11-14 show different simulation results for the second scenario where the SNR is fixed to -5, 0, 5 and 10 dB in Figures 11, 12, 13 and 14, respectively. It can be noticed from Figure 11 where the SNR is fixed to -5 dB and the number of rounds is changed from one to sixteen and the number of S-Boxes is changed from one to eight, that the SAC is only present when the number of rounds is between twelve and sixteen while the number of S-Boxes is at eight. It can be clearly noticed from Figures 11-14 that the probability of correct reception is improved when the number of S-Boxes and rounds decrease. While the probability of correct reception is enhanced significantly when the SNR is increased, which can be noticed in Figure 14, where the probability of correct reception is always equal to 1, due to the fact the SNR is equal to 10 dB. Therefore, we can also notice that when the channel conditions are perfect (i.e., $SNR \geq 10db$) the probability of correct reception is equal to one, for any number of rounds or S-Boxes. Figures 15-18 depict simulation results for the third scenario where the number of rounds is fixed and is equal to one, four, eight and twelve rounds in Figures 15, 16, 17 and 18, respectively. It can be noticed from Figure 15 where the number of rounds is fixed to one round and the number of S-Boxes is changed from one to eight and the SNR is changed from -5 to 20 dB, that the SAC is not present in this

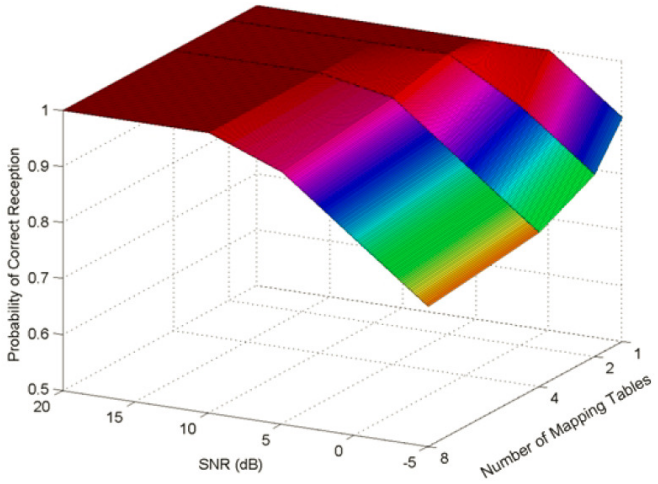


Fig. 15. The effect of the number of distinct S-Box mapping tables and SNR on the probability of correct reception for a fixed number of rounds equal to 1

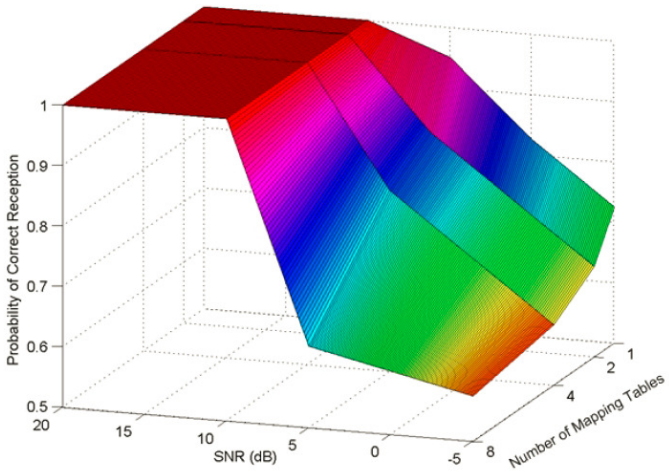


Fig. 17. The effect of the number of distinct S-Box mapping tables and SNR on the probability of correct reception for a fixed number of rounds equal to 8

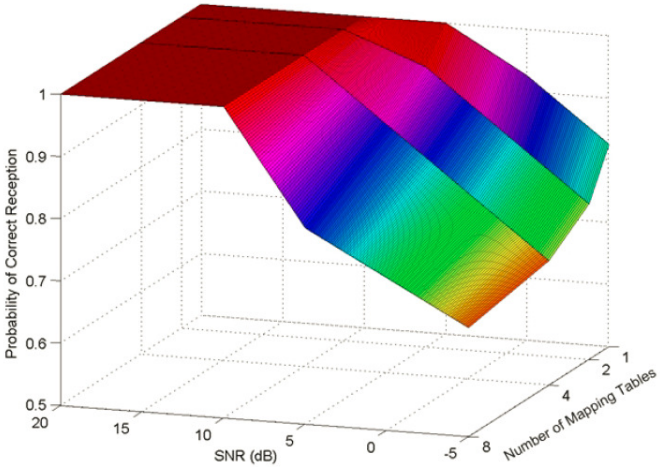


Fig. 16. The effect of the number of distinct S-Box mapping tables and SNR on the probability of correct reception for a fixed number of rounds equal to 4

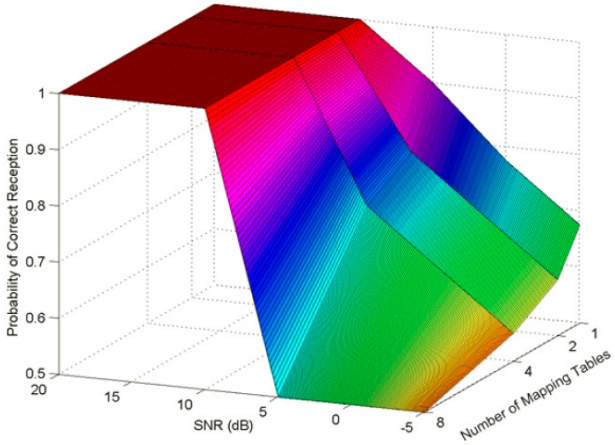


Fig. 18. The effect of the number of distinct S-Box mapping tables and SNR on the probability of correct reception for a fixed number of rounds equal to 12

case, due to the fact that the number of rounds is equal to the minimum. Similarly, when the number of round is equal to four and eight in Figures 16 and 17, the SAC is still not present. However, the SAC starts to show when the number of rounds is equal to 12. Therefore, we can conclude that that the SAC is not present in DES until the number of rounds is equal to 12 or more, regardless of the channel condition and the number of S-Boxes.

By the end of this section, we can notice from the three different simulation scenarios, that SAC is present only when the following three conditions are present all together

1. The number of S-Boxes is eight
2. The number of rounds is between 12 and 16
3. The SNR value is between -5 and 5 dB.

B. Error Performance of M-DES

By introducing round 17, reducing the number of S-Boxes and changing the design of the S-Box mapping tables in M-DES, the algorithm is shown to alleviate the SAC under all circumstances. The number of the S-Box mapping tables in M-DES is two. Therefore, by alternating the number of rounds in M-DES as well as changing the channel conditions (i.e., SNR of the channel), the probability of correct reception will be changed. However, when the number of rounds is changed, round 17 is still applied after the selected number of the original rounds to alleviate the SAC effect. To summarize, in this simulation the number of S-Boxes is fixed to two S-Boxes (M-DES number of S-Boxes) and the probability of correct reception is computed for every single value of SNR between –5 and 20 dB and for every different number of rounds between one and sixteen (with round 17 applied in all the cases). Table I summarizes the probability of correct reception for the case when the SNR is equal to -5 dB for different number of rounds from one to sixteen with round 17 applied in all cases.

It can be noticed from table I that the probability of correct reception in M-DES is significantly improved compared to that of DES for the same number of rounds, S-Boxes and SNR

Table I
The probability of correct reception for M-DES (2 S-Boxes) when the SNR is equal to -5 dB and the number of rounds is varied from one to sixteen, with round 17 applied in all cases of M-DES compared to the same scenario of DES with two S-Boxes only

Number of rounds	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
M-DES	0.9	0.89	0.88	0.87	0.86	0.85	0.84	0.83	0.81	0.8	0.78	0.77	0.77	0.77	0.77	0.77
DES	0.79	0.78	0.77	0.76	0.75	0.74	0.7	0.72	0.70	0.69	0.67	0.66	0.66	0.66	0.66	0.66

value. This improvement in the error performance is a result of the change in the S-Boxes design as well as to the addition of round 17.

Hence, in this section we show that the probability of correct reception in M-DES is a function of two variables, which are the number of rounds and the SNR. Moreover, we show that M-DES significantly improves the error performance compared to DES. In the next section, we show the effect of the number of rounds and S-Boxes on the security of the encrypted data. In addition, we evaluate the security addition of round 17 to M-DES.

IV. Effect of the Number of Rounds and S-Boxes on the Security

When the security of encryption algorithms is evaluated, two main attacks are considered. The Brute force attack where the key is attacked; and the differential or linear attacks where the actual data is attacked [6]. The number of rounds and S-Boxes does not have an effect on the brute force attack due to the fact that the brute force attack is an attack where all possible keys are tried in decryption to get the correct or expected plaintext. Moreover, the attacker who obtains a ciphertext tries all possible keys to decrypt the ciphertext he obtained, until he gets a plaintext that he expects out of the decryption process. The obtained key can be further used to decrypt all other ciphertext obtained by the attacker. However, the number of rounds and S-Boxes directly impacts the strength of the differential cryptanalysis attack due to the fact
that this attack is based on the confusion and diffusion of the data bits, which are mainly affected by the number of rounds and S-Boxes. Moreover, the attack assumes that the attacker already have access to a number of plaintexts and their associated ciphertexts without knowing the key by which they were encrypted. By having enough number of plaintexts and their associated ciphertexts, the attacker can study the relationship between each bit of the plaintext and each bit of the ciphertext. It is assumed that if the enough number of pairs to perform the attack is available, the attacker can obtain the key immediately. The complexity of the attack increases when the number of rounds increases and when the operations inside each round gets more complicated [9]. Therefore, the number of rounds and S-Boxes directly impacts the strength of the differential cryptanalysis attack.

A. Security of DES

In [9] it is shown that when 2^{47} pairs of plaintexts and their associated ciphertexts are available to the attacker, the key by which these pairs were encrypted can be immediately obtained. Table II summarizes the number of pairs required to break the standard DES when different number of S-Boxes and rounds are selected in DES. For example, if we take the case where two S-Boxes and sixteen rounds are selected, 2^{13} pairs of plaintext and their associated ciphertexts are enough to break the algorithm and discover the key, compared to the case where 2^{47} pairs are required to break the algorithm when eight S-Boxes and sixteen rounds are selected.

Table II
Number of pairs needed to crack DES using differential cryptanalysis for different number of rounds and S-Boxes in DES

Number of Rounds	1 S-Box	2 S-Boxes	4 S-Boxes	8 S-Boxes
2	2^0	2^0	2^2	2^3
4	2^0	2^1	2^3	2^5
6	2^1	2^2	2^5	2^8
8	2^2	2^4	2^8	2^{14}
10	2^3	2^7	2^{14}	2^{24}
12	2^4	2^9	2^{18}	2^{31}
14	2^5	2^{11}	2^{22}	2^{39}
16	2^6	2^{13}	2^{27}	2^{47}

Therefore, it can be noticed that increasing the number of rounds and S-Boxes enhances the security of the encrypted data. In our analysis, we assume that if the attacker has all the required pairs required to break the algorithm using the differential cryptanalysis attack, the algorithm can be broken in zero seconds, and the algorithm is no longer considered secure. Based on Table II, given that the combination of two rounds/one S-Box is the least secure and the combination of 16 rounds/8 S-Boxes is the most secure. Let's define a normalized (w.r.t. the most secure case) security level metric as follows

$$S_d = \frac{\log_2 N_p}{\log_2 N_{pm}} \qquad (1)$$

Where N_p is the number of pairs needed to break the algorithm for a given rounds/S-Boxes combination and N_{pm} is the maximum number of pairs needed to crack the algorithm in the most secure case, which is equal to 2^{47} pairs. Figure 19 shows the relationship between the number of rounds and the normalized security level S_d for different number of distinct S-Boxes (using Eq. 1). It can be noticed from the figure that the security is enhanced whenever the number of rounds or the number of S-Boxes increase. Therefore, the most secure case ($S_d = 1$) is when we have eight S-Boxes and 16 Rounds (original DES design), conversely the worst case

($S_d = 0$) is when we have one S-Box and one round only. However, DES with its original design (16 rounds and 8 S-Boxes) has been shown to be no longer considered secure [9], although we show later in this section that its modified version M-DES proposed in [5] solves its security problem.

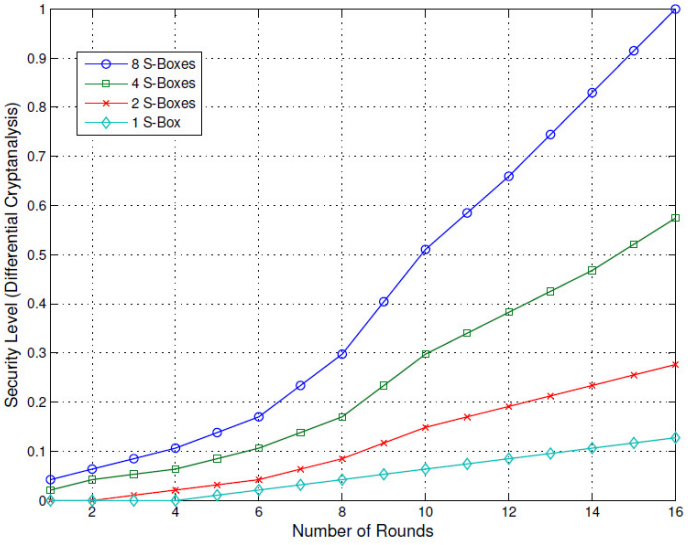


Fig. 19. The relationship between the number of rounds and the security level for different number of distinct S-Boxes

B. *Security of M-DES*

The encryption algorithm proposed in [5] alleviates the SAC by reducing the number of S-Boxes from eight to two in addition to modifying the design of their mapping tables as well as the addition of round 17. However, to overcome the security reduction due to the dropping of six S-Boxes, the authors introduced a new round with a new key as shown earlier in Figure 5. In original DES as shown in the previous table, 2^{13} pairs of plaintext and their associated ciphertext are required to attack the algorithm when two S-Boxes and sixteen rounds are chosen. However, by the introduction of round 17, the existence and availability of those pairs is not enough to break the algorithm and obtain the key. This is due to the fact that the differential cryptanalysis on DES requires both the plaintext and the ciphertext to be of a length equal to 64 bits. However, in M-DES, the 64-bit cipher is hidden in a larger 128-bit key. Therefore, assuming that 2^{13} pairs of 64-bit plaintexts and their associated 128-bit M-DES ciphertext are available to the attacker, the attack can't be directly applied until the actual 64-bit cipher is extracted from each 128-bit cipher. Hence, a new security measure can be defined by the time required to attack the algorithm. Assuming that the required pairs are available and already extracted, it is further assumed that the key is obtained immediately. Round 17 in M-DES adds an additional time overhead to perform the attack, which is the time required to extract the 64-bit useful ciphers from each 128-bit cipher and is called t_1. We find t_1 for all the cases described in Table II. Assuming that the number of pairs given in an entry of Table II is called N_P, therefor the time t_1 is given by

$$t_1 = \frac{(N_1)^{N_P}}{N_2}, \tag{2}$$

Where N_1 is the number of operation needed to extract one useful 64-bit cipher out of one 128-bit cipher, which is given by

$$N_1 = \binom{32}{16} \times 16! = 1.276 \times 10^{22} \ trials \tag{3}$$

and \$N_2\$ is the number of operations that can be performed during one second by the microprocessor. Therefore, Eq. 2 can be given by

$$t_1 = \frac{(1.276 \times 10^{22})^P}{N_2} \tag{4}$$

As a case study, if we take a super computer that is able to run 2.5×10^{12} operations per second, eq. 4 can be given by

$$t_1 = \frac{(1.276 \times 10^{22})^P}{2.5 \times 10^{12}} \tag{5}$$

for example, if we take the case where we have 10 rounds and 4 S-Boxes, $N_p = 2^{14}$ pairs of plaintext and their associated ciphertexts are required to crack the algorithm, however the useful 64-bit ciphertext need to be extracted out of each 128-bit ciphertext. Hence the time (in seconds) to extract all the useful 64-bit ciphertexts is given by

$$t_1 = \frac{(1.276 \times 10^{22})^{2^{14}}}{2.5 \times 10^{12}} = 7.236 \times 10^{362169} \tag{6}$$

Another metric that can be used to evaluate the security is the probability of attack given that all the required pairs are available (before the extraction of the useful ciphertexts), this probability is assumed to be equal to 1 without the use of round 17 (no ciphertext extraction is required). The probability of extracting one useful ciphertext out of a 128-bit cipher is given by

$$p_1 = \frac{1}{\binom{32}{16} \times 16!} = 7.9515 \times 10^{-23}. \tag{7}$$

The experiment of guessing the useful ciphers and their correct order for all the N_p pairs in M-DES is a Bernoulli trial (repeating the experiment N times out N_p ciphers). Hence, the probability of a successful attack on M-DES using differential cryptanalysis is given by

$$P_{attack} = \binom{N_P}{N_P} p_1^{N_P} (1 - p_1)^{N_P - N_P} = p_1^{N_P} = (7.9515 \times 10^{-23})^{N_P}. \tag{8}$$

Therefore, the probability of attack decreases when the number of pairs required in Table II increase (increased number of rounds and S-Box mapping tables). For example if we take the

Table III
The probability of extracting all 64-bit ciphertext from the 128-bit ciphertext of M-DES in [5]

N_r	1 S-Box	2 S-Boxes	4 S-Boxes	8 S-Boxes
2	7.9515×10^{-23}	7.9515×10^{-23}	$(7.9515 \times 10^{-23})^4$	$(7.9515 \times 10^{-23})^8$
4	7.9515×10^{-23}	$(7.9515 \times 10^{-23})^2$	$(7.9515 \times 10^{-23})^8$	$(7.9515 \times 10^{-23})^{32}$
6	$(7.9515 \times 10^{-23})^2$	$(7.9515 \times 10^{-23})^4$	$(7.9515 \times 10^{-23})^{32}$	$(7.9515 \times 10^{-23})^{128}$
8	$(7.9515 \times 10^{-23})^4$	$(7.9515 \times 10^{-23})^{16}$	$(7.9515 \times 10^{-23})^{128}$	$(7.9515 \times 10^{-23})^{2^{14}}$
10	$(7.9515 \times 10^{-23})^8$	$(7.9515 \times 10^{-23})^{128}$	$(7.9515 \times 10^{-23})^{2^{14}}$	$(7.9515 \times 10^{-23})^{2^{24}}$
12	$(7.9515 \times 10^{-23})^{16}$	$(7.9515 \times 10^{-23})^{512}$	$(7.9515 \times 10^{-23})^{2^{18}}$	$(7.9515 \times 10^{-23})^{2^{31}}$
14	$(7.9515 \times 10^{-23})^{32}$	$(7.9515 \times 10^{-23})^{2^{11}}$	$(7.9515 \times 10^{-23})^{2^{22}}$	$(7.9515 \times 10^{-23})^{2^{39}}$
16	$(7.9515 \times 10^{-23})^{64}$	$(7.9515 \times 10^{-23})^{2^{13}}$	$(7.9515 \times 10^{-23})^{2^{27}}$	$(7.9515 \times 10^{-23})^{2^{47}}$

same case we discussed earlier of the 10 rounds with four S-Boxes, the probability of attacking the algorithm (extracting all useful ciphertexts) is given by

$$P_{attack} = (7.9515 \times 10^{-23})^{N_P} \qquad (9)$$

which is a very small probability. Table III summarizes the probability of attack for all cases described in Table II.

To summarize, in this section we have shown that the security of the encrypted data decreases when the number of rounds and S-Boxes decreases. We also showed that the addition of round 17 in M-DES [5] significantly improves the security by increasing the time required for a successful attack which implies a very low probability of successful attack on M-DES. In addition, we evaluated the security enchantment of the new round proposed in M-DES in a more comprehensive way, where we numerically evaluated the probability of a successful attack on the proposed algorithm as well as calculating the time required for such an attack.

V. Conclusions

In this paper we evaluated the effect of the number of rounds and the number of S-Boxes on the probability of correct reception assuming different channel conditions. In addition, we also evaluated the effect of the number of rounds and the number of S-Boxes on the security level of the encrypted data in DES as well as in M-DES. We have shown that the probability of correct reception is improved when the number of rounds and S-Boxes is decreased. Moreover, we have shown that the security of the encryption algorithm is enhanced when the number of rounds and S-Boxes is increased. We have also evaluated the security enhancement of the new round proposed in M-DES in a more comprehensive way, where we numerically evaluated the probability of a successful attack on the proposed algorithm as well as calculating the time required for such an attack. We have shown that the time to achieve a successful attack on M-DES is tremendously high given that a very fast super computer is used in the attack, which implies an insignificant probability of such an attack on M-DES.

References

[1] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM Journal of Research and Development,* vol. 38, no. 3, pp. 243-250, 1994.

[2] M. Matsui, "On correlation between the order of S-boxes and the strength of DES", *in Proceedings of Eurocrypt'94, Lecture Notes in Computer Science* vol. 950, pp. 366-375, Springer-Verlag, 1995.

[3] D.W. Davies and S. Murphy, "Pairs and triplets of DES S-Boxes," *Journal of Cryptology*, vol. 8, pp. 1-25, 1995.

[4] Hui Shi, " Analysis of the avalanche effect of the AES S box," *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*, Zhengzhou, China, August, 2011.

[5] W. Zibideh and M. Matalgah, "Modified Data Encryption Standard with Improved Error Performance and Enhanced Security in Wireless Communication Channels," *2011 IEEE Radio Wireless Symposium*, Phoenix, AZ, Jan 2011.

[6] Behrouz A. Forouzan, *Cryptography and Network Security*. First Edition, Mc Graw Hill, 2008.

[7] W. Stallings, *Cryptography and Network Security, Principles and Practice*. First Indian Edition, Pearson Educational, 2003.

[8] National Institute for Standards and Technology, Data Encryption Standard (DES), FIPS 46-3, US Department of Commerce, May, 1999.

[9] E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-Round DES," *Advances in Cryptology CRYPTO 92, Lecture Notes in Computer Science*, vol. 740, pp. 487-496, Springer-Verlag, 1993.

Walid Y. Zibideh received his bachelor degree in Computer Engineering from Jordan University of Science and Technology in 2007. He obtained the Masters degree in Electrical Engineering from the University of Mississippi in 2010. He is currently working toward the Ph.D degree in Electrical Engineering at the University of Mississippi and is expected to graduate in August 2012. Since February 2012, he joined Qualcomm as a power management Test Engineer. His research interest includes Security and Power Management techniques. He is the recipient of the best paper award in the 2011 IEEE Radio Wireless Week in Phoenix, AZ, USA.

Mustafa M. Matalgah received his Ph.D. in Electrical and Computer Engineering in 1996 from The University of Missouri, Columbia. From 1996 to 2002, he was with Sprint Corp., Kansas City, Missouri, where he held

various technical positions leading a wide range research and development projects dealing with the evaluation and assessment of 3G wireless communication emerging technologies for the Next Generation Networks (NGNs). Since August 2002, he has been with The University of Mississippi in Oxford where he is now an Associate Professor of Electrical Engineering. He had been invited and served as a Visiting Professor at Chonbuk National University in South Korea and at Misr International University (MIU) in Egypt. His current technical and research experience is in the fields of performance evaluation and optimization of emerging wireless communications systems in fading channels. He has published more than 100 refereed journal and conference proceeding papers, two books, five book chapters, and more than 20 technical industrial applied research reports in these areas. Dr. Matalgah received several certificates of recognition for his achievements in the industry and academia. He is the recipient of the Faculty Best Paper Award of the IEEE ISCC 2005 Conference, La Manga del Mar Menor, Spain and a co-recipient of the Student Best Paper Award of the IEEE RWS 2011 Conference, Phoenix, AZ, USA. He is also the 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, serves as reviewer for several international journals and conferences, and served on several international conferences technical program and organizing committees.