S-DES: An Efficient & Secure DES Variant

Mohamad Noura[1], Hassan N. Noura[2], Ali Chehab[2], Mohammad M. Mansour[2] and Raphaël Couturier[1]

[1]FEMTO-ST Institute, Univ. Bourgogne Franche-Comté (UBFC), France
[2] American University of Beirut, Electrical and Computer Engineering, Lebanon

***Abstract*—In this paper, we propose an efficient and secure variant of DES (S-DES), which strikes a good balance between performance and security level when compared to 3DES. S-DES is based on the same round function of DES, however, we introduce different modifications to overcome the weaknesses of the original DES such as the extended Feistel Network (FN) instead of the FN. The main advantage of the proposed scheme is that it benefits from the cryptographic characteristics of DES substitution and diffusion primitives. However, the size of the secret key is extended to 112 bits and the data block is set to 128 bits, which provides better resistance against the attacks that plagued DES. Moreover, the proposed internal scheme of S-DES allows for a parallel implementation, which reduces the response latency. Finally, the main idea of this paper is not to provide a better alternative to the existing standard (AES), but to provide an efficient candidate solution from the well-optimized DES cipher.**

***Index Terms*—Secure variant of DES; Extended Feistel Networks; Security and performance analysis;**

I. Introduction

Information security is a mandatory feature for all types of networks. Information security can be ensured by employing cryptographic or non cryptographic solutions. Cryptographic solutions provide protection against confidentiality, integrity, and source authentication threats. While the availability threat requires non-cryptographic solutions such as Firewalls and intrusion detection/prevention systems.

In this paper, we focus on the confidentiality threat that presents itself in the form of eavesdropping and traffic analysis. To resist this kind of a threat and ensure Data Confidentiality (DC), the use of an encryption algorithm is mandatory. This preserves the secrecy of the transmitted data between two peers communicating over an insecure channel or for storing data under a non-trusted system such as a cloud.

The structure of current block ciphers consists of applying a round function [1] for several rounds (r). Two kinds of round functions can be employed, the Feistel Network (FN) that is used in the Data Encryption Standard DES [2] or the Substitution-Permutation Network (SPN) that is used in AES [3], which replaced DES in the year 2000.

A. Related Works

DES was developed by IBM and it was based on the Lucifer cipher. It was standardized in 1977 by the National Bureau of Standards (NBS). The design criteria for DES were not published and some modifications were introduced, which reduced the security level of DES such as reducing the size of the secret key from 128 to 56 bits. This modification was the reason behind breaking DES after 20 years!

More importantly, DES was extensively studied in the last 30 years since it was the first standard symmetric encryption algorithm. Previously, DES was demonstrated that it is quite robust against known analytical attacks such as **linear, differential attacks[4], chosen/known-plain-text, cipher-text-only, and statistical attacks in addition to resisting brute force attacks**. However, from the mid-1990, DES with a 56-bit key size could be easily broken through an exhaustive key search [1]. To overcome this issue, a solution was presented and consisted of applying DES for three times and this solution was called 3DES [2]. This solution allows for the use of two or three different keys to make the complexity of brute force attacks at least 2^{112}, which is much harder to be break compared to a complexity of 2^{56}. 3DES [5] was presented to achieve a higher security but unfortunately introduced an important overhead, which is the cost of triple encryption/decryption, which tripled the required resources and latency. In addition, 3DES was not suitable for real-time applications or to be used on tiny devices[6].

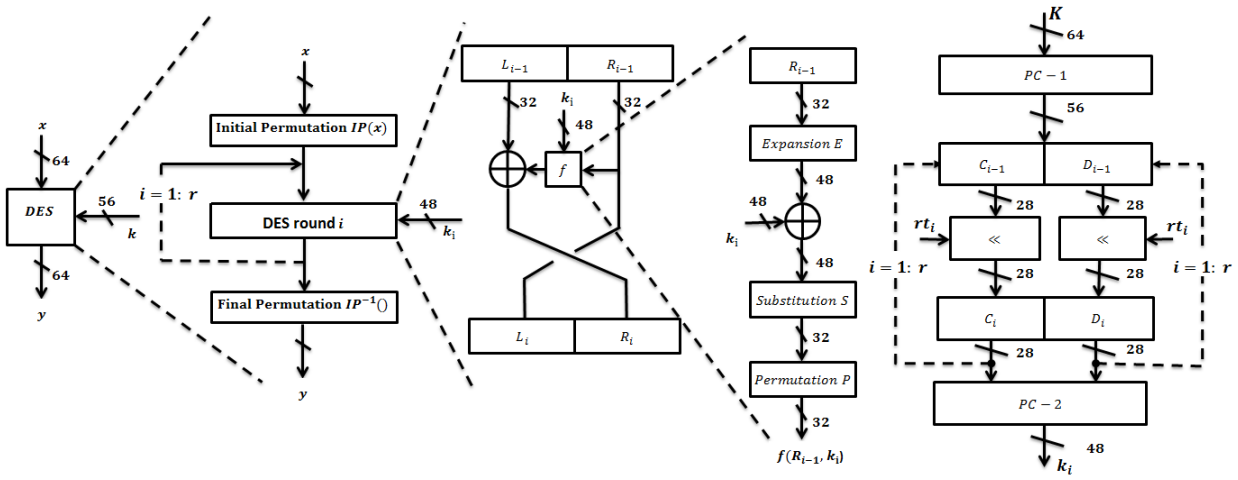
B. Motivations and Contributions

DES and 3DES are still widely used today in different industrial applications, mainly because the DES implementation was highly optimized in addition to the high cost of modification. As such, defining a new variant of DES would be welcomed in part of the industrial field. **The main goal of this paper is to propose a new secure variant of DES that can overcome the existing DES attacks. Equally important, the proposed variant should ensure a low execution time compared to 3DES.**

C. Proposition and Advantages

The proposed scheme reduces the computational complexity as compared to 3DES, while ensuring resistance against analytical and brute force attacks. Moreover, its execution time is similar to DES since the proposed variant uses the DES round function with a slightly different operation. Moreover, the internal structure of the proposed variant can ensure parallel computations, which reduces the required latency. Therefore, the proposed variant solves the security issues of DES and the performance limitations of 3DES. Experimental results prove

978-1-5386-1254-5/18/$31.00 ©2018 IEEE



(a) DES (b) DES key schedule

Fig. 1: Structure of DES and its corresponding key schedule.

the efficiency of the proposed variant and its robustness as compared to DES and at least 2 times faster than 3DES [7], [8]. On the other hand, several security tests were performed to validate that the proposed cipher ensures the avalanche effect, key sensitivity, and a high level of randomness.

D. Organization

The rest of this paper is organized as follows: DES and its corresponding variants are presented in Section II. In Section III, the details of the proposed algorithm as well as the functionality of each operation are described. Then, a security analysis and cipher performance tests are presented in Section IV and V, respectively. Finally, conclusion and future works are presented in Section VI.

II. Introduction of DES Algorithm and its Variants

DES uses the classic uniform Feistel Network and has a block size of 64 bits and a key size of 56 bits (see Fig.1-(a)). The secret key consists of eight bytes, however, one bit of each byte is dropped, which means that the key size is effectively 56 bits. The input block (64 bits) is separated into 2 sub-blocks (words): the 32 leftmost bits part L and the 32 rightmost parts R. Then, the round function is applied 16 times and for each round a new L and R are produced as defined in the following:

$$\begin{aligned} R_i &= f(R_{i-1}, k_i) \oplus L_{i-1} \\ L_i &= R_{i-1} \end{aligned} \tag{1}$$

Where $i = 1, 2, \ldots, 16$, and k_i stands for the i^{th} round key. The set of round keys is generated from the secret key, K. Fig. 1-(b) illustrates the DES key schedule. In fact, any slight modification to k should produce a different set of round keys.

As DES is based on the Feistel structure, the encryption and decryption differ only in key-schedule. It starts with a Bit-wise initial permutation, then 16 rounds are applied. The steps are summarized as follows:

- Plain-text block is split into 32-bit halves L_{i-1} and R_{i-1}.
- R_{i-1} is introduced into the function f, the output of which is then XOR-ed with L_{i-1}.
- Left and right halves are swapped.
- After the 16^{th} round, L_{16} and R_{16} are swapped again followed by a final permutation.

The main issue of DES is the effective key size (56 bits), and the total key space of 2^{56}. For the first twenty years, the DES algorithm could not be broken. However, In 1999, EFF broke the challenge by a brute-force attack just within 22.25 hours [1].

A. DES Round function (f)

The DES round Function is the main operation of DES. its inputs are: R_{i-1} and round key k_i. The four operations of f are:

- **Expansion** (E): Its main purpose is to increase diffusion property by duplicating 12 specific bits.
- **Addition Round Key**: "Exclusive or" between the i^{th} round key (k_i) and the output of the expansion function E (R_{i-1}). The round keys k_i, $i = 1, \ldots, r$ are obtained from the DES key schedule that requires the secret key K.
- **Substitution** S: Eight substitution tables are employed. 6 bits are used for inputs, and 4 bits are produced as an output from every $S-box$. The $S-boxes$ are nonlinear transformations and ensure resistance against analytical attacks. In fact, it can be considered as the most crucial operation.
- **Permutation** P: It is a bit-wise permutation that introduces diffusion. The output bits of one S-Box affect several S-Boxes in the next round.

As a conclusion, E and P ensure the diffusion property, while the substitution S ensure the confusion property. In

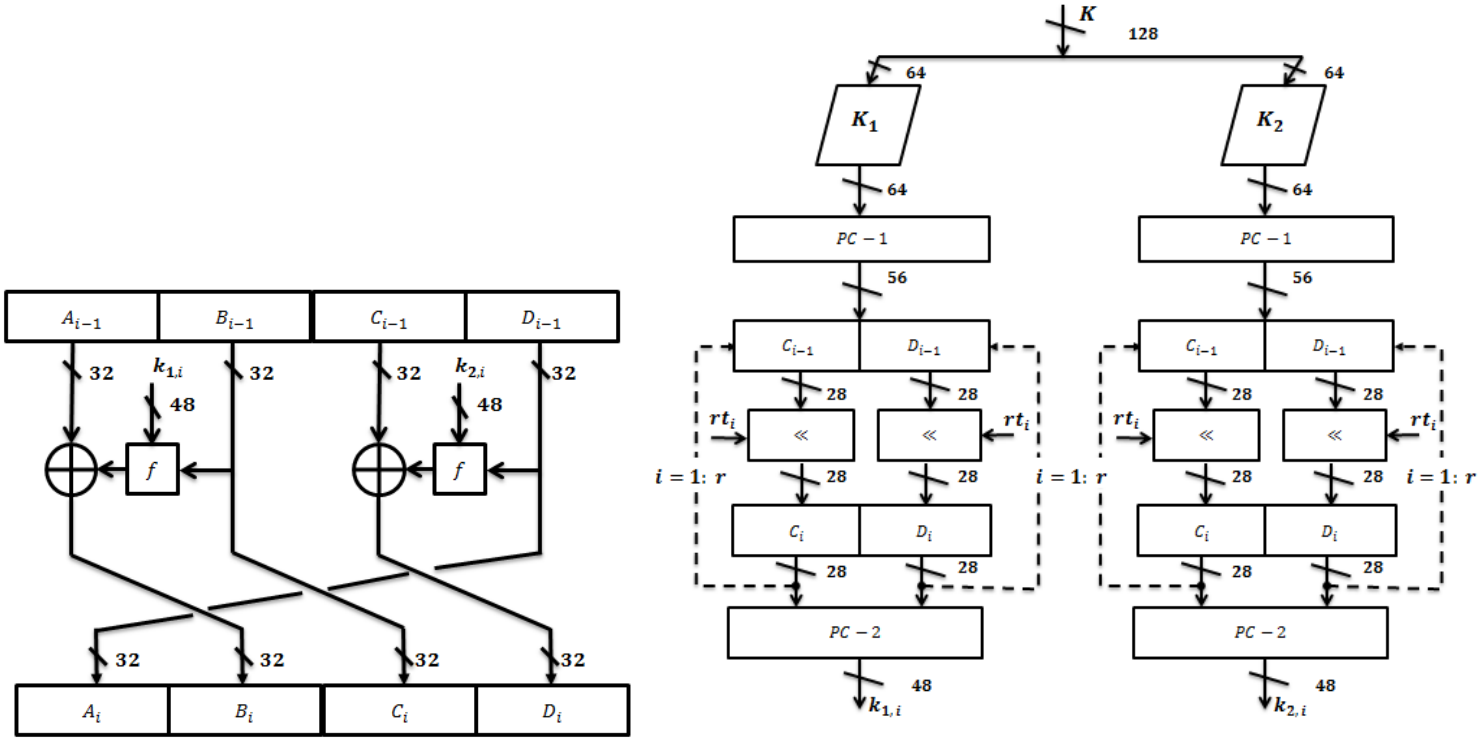


Fig. 2: The proposed round Structure of S-DES and its corresponding key schedule.

addition, the avalanche effect and key sensitivity are achieved starting from the 5^{th} round.

B. DES Key Schedule

The input to the DES key schedule algorithm is a secret key with 64 bits: 56 bits key and 8 bits parity. Parity bits are removed in a first permuted choice PC_1. It is important to note that the parity bits are not used at all during the generation process of the round keys. Then, the output is split into 28-bit halves C_0 and D_0. In round $i = 1,\ 2,\ 9,\ 16$, the two halves are each rotated left by one bit. While, for the other rounds, the two halves are each rotated left by two bits. For each round, permuted choice PC_2 selects a permuted subset of 48 bits of the concatenation of C_i and D_i as round key k_i. Therefore, the output of the DES key schedule algorithm is 16 round keys (or sub-keys) k_i, where each one has a length of 48 bits and can be considered as a permutation of K.

On the other hand, the key schedule has to be modified for the decryption process. In fact, by using the same secret key, the same 16 round keys will be produced, but they are used in a reverse order. As $D_0 = D_{16}$ and $C_0 = C_{16}$, the first round key can be generated by applying PC_2 right after PC_1 (no rotation in round 1). All other rotations of C and D can be reversed to reproduce the other round keys resulting in:

1) One bit rotation to the right in rounds 2, 9 and 16.
2) Two bit rotations to the right in all other rounds.

C. Variant of DES: 3DES

Even though the DES algorithm had security weaknesses, some alternatives were proposed based on the DES algorithm [9]. One alternative is triple DES, often denoted as 3DES [2]. 3DES means Triple encryption using DES, as shown in the following equation:

$$y = DES_{k3}(DES_{k2}(DES_{k1}(x))) \tag{2}$$

3DES extends the effective key size to 112 compared to DES. Therefore, triple DES seems resistant to both exhausted key search and analytical attacks. Another version is triple DES, expressed as:

$$y = DES_{k3}(DES^{-1}_{k2}(DES_{k1}(x))) \tag{3}$$

The advantage here is that this version only performs single DES encryption if $k_1 = k_2 = k_3$. Triple DES is efficient when implemented in hardware but not when implemented in software. Another disadvantage for 3DES is the short block size of 64 bits, which is not suitable for some applications. Since Triple DES is resistant to exhausted key search and analytical attacks, it is still being used in many legacy applications including the banking sector.

III. Proposed S-DES Variant

In this section, a secure and efficient DES variant (S-DES) is proposed towards ensuring better resistance against attacks without degrading the performance.

A. Encryption/Decryption Algorithm

The S-DES algorithm has a key size of 128 bits, from which only 112 bits are used after removing the parity bits. The input data block includes 128 bits, and it is divided into 4 sub-blocks (A, B, C, D) each of size 32 bits as shown in Fig. 2-(a). The proposed round function can be expressed as:

$$B_i = f(B_{i-1}, k1_i) \oplus A_{i-1}$$
$$D_i = f(D_{i-1}, k1_i) \oplus C_{i-1} \quad (4)$$

S-DES iterates the round function 16 times, but with extended FN (4 sub-blocks instead of 2), where each couple uses a different key schedule.

Note that at the end of each round, a right rotation operation is realized on the output (A_i; B_i; C_i; D_i), which become (B_i; C_i; D_i; A_i). The pseudo-code of the proposed S-DES encryption algorithm is listed in Algorithm 1. The decryption algorithm is the same as encryption, but the order of round keys is reversed.

B. Proposed S-DES Key expansion

The proposed key generation algorithm can be seen in Fig. 2-(b) and is described in the following steps:
The permutation tables of DES IP and IP^{-1} are preserved in our proposal. The input key which is improved from 64 bits to 128 bits is then divided into 64 bits each, resulting in $K = K_1||K_2$. According to the key scheduling of the DES, K_1 is on the left side and K_2 is on the right side, each has an output of 56 bits after removing 8 parity bits, through the permuted choice-1 (PC-1). Each K_j with a length of 56 bits is processed as in DES key schedule to produce the j^{th} ($j = 1$ or 2) set of round keys ($RK_j = RK_{j,1}, RK_{j,2}, \ldots, RK_{j,16}$).

Two sets of round keys are produced, where each one contains r sub-keys: $\{RK_{1,1}, RK_{1,2}, \ldots, RK_{1,r}\}$ use on the left side, while $\{RK_{2,1}, RK_{2,2}, \ldots, RK_{2,r}\}$ use on the right side. More details about the S-DES key expansion algorithm of S-DES is presented in Algorithm 1.

IV. Security Analysis

There are several tests that can permit to quantify the robustness of ciphers. The proposed S-DES variant should be strong enough to guard against the most known types of attacks such as statistical, differential, chosen/known plain-text, and brute-force attacks [1]. Extensive experiments are performed in this section to demonstrate the efficiency and high security level of the proposed scheme against these well-known attacks. In the following, several metrics are analyzed towards verifying the cryptographic strength of the proposed variant. In fact, doubling the size of the data block and the secret key doubles its resistance against analytical and brute force attacks. In the following tests, 1,000 original random plain blocks are generated following a normal distribution with a mean equals to 128 and standard deviation close to 16.

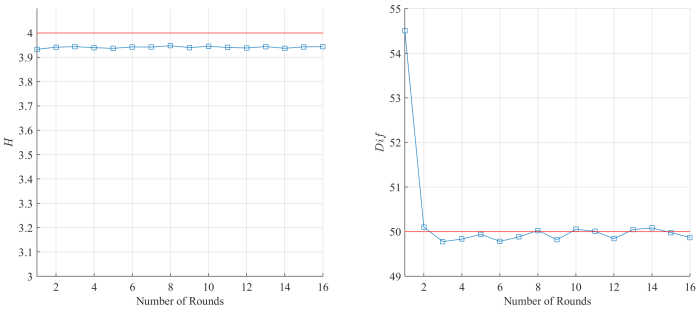
A. *Statistical Analysis*

To resist statistical attacks, the cipher must exhibit some randomness properties [1], which can be assessed via several statistical security tests such as a) the Entropy analysis and b) the difference between plain and cipher texts.

*1) **Uniformity Analysis: Information Entropy Analysis**:* An important randomness property is the uniformity property that can be quantified by measuring the entropy of the encrypted sequence, and it should have a maximum value. The average entropy variation of the encrypted blocks is shown in Fig. 3-(a) for 1,000 random secret keys and as a function of the number of rounds. It is shown that the encrypted blocks always have an entropy close to the desired value of 4 ($\log_2(16) = \log_2(2^4) = 4$) for a block size of 16 bytes. Accordingly, the uniformity of the proposed cipher, S-DES, is confirmed.

B. *Independence: Difference Between Plain and Cipher texts*

The encrypted blocks must be largely different from the original ones, by at least 50% at the bit level. The variation of the difference between plain and encrypted blocks is shown in Fig. 3-b versus the round number. The results show that at least 50% of the block has been changed after encryption from the 6^{th} round. Therefore, the proposed variant reaches a high difference value between original and encrypted blocks, which means that it can ensure the independence property. Consequently, the randomness property is confirmed since the uniformity and the independence properties are satisfied.



(a) Entropy (H) versus rounds (b) Difference (Dif) versus rounds

Fig. 3: (a) Variation of the entropy of the encrypted blocks and (b) the difference between original and encrypted blocks versus the number of rounds r and for 1,000 random secret keys with r=16.

C. Sensitivity Tests

The sensitivity test shows how much would a slight change in the plain-text or in the key affect the resulted cipher text. In this context, the higher the encryption change, the better the sensitivity of the encryption algorithm. Below, we analyze the sensitivity of the proposed approach concerning both, the plain-text change and the key change.

Algorithm 1 Proposed S-DES Algorithm and its Key Schedule Algorithm.

S-DES Encryption Algorithm

procedure S-DES(M, K)
  Input: Plain-text stored in four w-bit input registers A; B ; C; D
  Number r of rounds
  $2 \times w$-bit round keys $k_1[1 \ \ldots, \ r]$ and $k_2[1, \ \ldots, \ r]$
  Output: Cipher-text stored in A; B ; C; D
  $M1 \leftarrow MSB(M, 64)$
  $M2 \leftarrow LSB(M, 64)$
  $M1 \leftarrow IP(M1)$
  $M2 \leftarrow IP(M2)$

  $A \leftarrow MSB(M1, 32)$
  $B \leftarrow LSB(M1, 32)$
  $C \leftarrow MSB(M2, 32)$
  $D \leftarrow LSB(M2, 32)$

  for $round \leftarrow 1$ to 16 **do**
    $K_{1,\,i}||K_{2,\,i} \leftarrow SK - SDES(K, \ round)$
    $A \leftarrow A \oplus f(B, \ K_{1,\,i})$
    $C \leftarrow C \oplus f(D, \ K_{2,\,i})$
    $(A; B; C; D) \leftarrow (B; C; D; A)$

  $(A; B; C; D) \leftarrow (B; C; D; A)$
  $M1 \leftarrow IP^{-1}(M1)$
  $M2 \leftarrow IP^{-1}(M2)$
  return M

S-DES Key Schedule Algorithm

procedure SK-SDES(K)
  Input:
  K: 128-bit key
  $PC1$: Permuted choice 1
  $PC2$: Permuted choice 2
  $r1, r2, ..., r16$: left shifts (rotations)

  Output:
  $K_1 = \{k_{1,\,1}, \ k_{1,\,2}, \ ..., \ k_{1,\,r}\}$: 16×48-bit round keys
  $K_2 = \{k_{2,\,1}, \ k_{2,\,2}, \ ..., \ k_{2,\,r}\}$: 16×48-bit round keys
  $k1 \leftarrow MSB(k, 64)$
  $k2 \leftarrow LSB(k, 64)$
  $K_1^{'} \leftarrow PC1(K1)$
  $K_2^{'} \leftarrow PC1(K2)$
  $r \leftarrow \{1, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1\}$
  $U \leftarrow MSB(K_1^{'}, \ 28)$
  $V \leftarrow LSB(K_1^{'}, \ 28)$
  $Z \leftarrow MSB(K_2^{'}, \ 28)$
  $W \leftarrow LSB(K_2^{'}, \ 28)$
  for $round \leftarrow 1$ to 16 **do**
    $U \leftarrow U << r_i$
    $V \leftarrow V << r_i$
    $Z \leftarrow Z << r_i$
    $W \leftarrow W << r_i$
    $k_{1,\,i} \leftarrow PC2(U||V)$
    $k_{2,\,i} \leftarrow PC2(Z||W)$
  return $k_{1,\,i}$ and $k_{2,\,i}, \ i = 1, 2, \ldots, r$

TABLE I: Statistical sensitivity results for (a) 3DES and (b) S-DES, for 1,000 random keys.

3DES				
	Min	Mean	Max	Std
Dif	49.69	50.001	50.23	0.0471
KS	49.932	49.99	0.0501	0.0199
$H-E$	5.73	5.763	5.7678	0.005

S-DES				
	Min	Mean	Max	Std
Dif	49.8859	50.0017	50.1239	0.0346
KS	49.9012	49.9990	50.0941	0.0333
$H-E$	5.7623	5.7657	5.7691	0.0012

*1) **Key Sensitivity test**:* It is one of the most important tests and it quantifies the sensitivity against a slight change in the secret key.

To study the key sensitivity, two secret keys K and K' are used, whereby K' differs by only one random bit from K. Two plain-texts are encrypted separately, and then, the Hamming distance (in bits) between the two cipher-blocks is calculated as follows:

$$KS = \frac{\sum_{k=1}^{T} dec2bin(E_K(P)) \oplus dec2bin(E_{K'}(P))}{T} \times 100\%$$

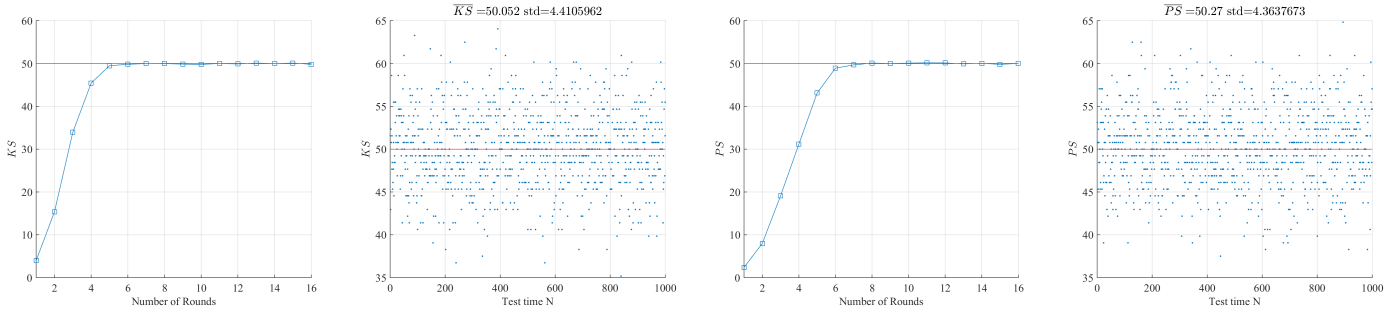
Where T is the length in bits of the data block. Fig. 4-(a) shows the variation of the key sensitivity versus the round number r. Based on the results, the key sensitivity is verified starting from the 6^{th} iteration with a difference of 50 bits. Also, we show in Fig. 4-(b) the key sensitivity for full S-DES repeated for 1,000 random keys and the results indicate a mean of 50, which confirms the high key sensitivity. Hence, the proposed system shows similar key-sensitivity when compared to the original DES and 3DES ciphers.

The statistical Results are shown in Table I (KS).

*2) **Plain-text Sensitivity**:* In this test, two plain-text $P1$ and $P2$ that are different by only one bit are encrypted separately to produce two cipher-texts $C1$ and $C2$. The plain-text sensitivity is computed according to the following equation:

$$PS = \frac{\sum_{k=1}^{T} dec2bin(E_K(P_1)) \oplus dec2bin(E_K(P_2))}{T} \times 100\%$$

Fig. 4-(c) shows the variation of the plain-text sensitivity versus the round number r. The results are similar to the key sensitivity; the plain-text sensitivity is achieved starting from the 6^{th} iteration. In addition, the results of the plain-text sensitivity for full S-DES, repeated 1,000 times, are shown



(a) KS versus the number of rounds (b) KS with r =16 (c) PS versus the number of rounds (d) PS with r =16

Fig. 4: Variation of the avalanche effect versus the number of rounds r (a) and for 1000 random secret keys with r =16 (b).In addition, variation of the key sensitivity versus the number of rounds r (c) and for 1000 random secret keys with r =16 (d)

in Fig. 4-(d). The resultant mean value is close to 50%, which means that with any one-bit change in the plain-text, results in more than 50% change in the corresponding cipher-text. Hence, the proposed approach ensures high plain-text sensitivity.

D. Discussion and Cryptanalysis: Resistance against the well-known types of attacks

The proposed variant (S-DES) ensures immunity against statistical, chosen/known plain text attacks since it exhibits good statistical performance verified through uniformity and independence, in addition to key and plaintext sensitivity. Furthermore, the complexity against differential and linear attacks has been doubled, and the complexity of the brute force attacks has been exponentially doubled. Accordingly, S-DES can resist the various well-known attacks.

V. Cipher Performance

The proposed S-DES was compared to DES and 3DES that is adopted in numerous open standards such as IPsec and TLS. The average encryption time between the proposed cipher (S-DES) and DES is computed for 100,000 times for an input block of 128 bits (one block for S-DES and 2 blocks for DES) without parallel computing. The results indicate that the proposed secure scheme requires the same time as DES and less than 2 times that of 3DES. This variant can benefit from the previous optimization of DES in both software and hardware implementations.

VI. Conclusion and Perspectives

The original DES cipher scheme suffers from several security weaknesses, while 3DES suffers from performance issues. This motivated the work to define a new efficient and secure DES variant, S-DES. Indeed, the newly proposed variant employs an extended FN with a 128-bit block size. In addition, the size of the secret key of S-DES is 112-bits. Therefore, S-DES provides better resistance against attacks such as brute-force, differential, and linear cryptanalysis. Furthermore, the desirable cryptographic performance is validated such as the avalanche effect, key sensibility, and high level of randomness degree with an acceptable trade-off between security and latency compared to the existing standards of DES and 3DES. Moreover, the proposed variant has been investigated with all possible cryptanalysis tests and attacks that are essential for any cipher algorithm to prove its credibility and robustness. Finally, the execution time of the proposed cipher is lower compared to 3DES.

References

[1] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[2] PUB FIPS. 46-3: Data encryption standard (des). *National Institute of Standards and Technology*, 25(10):1–22, 1999.

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

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round des. In *Differential Cryptanalysis of the Data Encryption Standard*, pages 79–88. Springer, 1993.

[5] Phil Karn, William Allen Simpson, and Perry Metzger. The esp triple des transform. 1995.

[6] Yongcheng He and Shuguo Li. A 3des implementation especially for cbc feedback loop mode. In *Circuits and Systems (ISCAS), 2017 IEEE International Symposium on*, pages 1–4. IEEE, 2017.

[7] Priyadarshini Patil, Prashant Narayankar, DG Narayan, and SM Meena. A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish. *Procedia Computer Science*, 78:617–624, 2016.

[8] Yang Jun, Li Na, and Ding Jun. A design and implementation of high-speed 3des algorithm system. In *Future Information Technology and Management Engineering, 2009. FITME'09. Second International Conference on*, pages 175–178. IEEE, 2009.

[9] Valerie Nachef, Jacques Patarin, and Emmanuel Volte. Des and variants: 3des, des–x. In *Feistel Ciphers*, pages 157–176. Springer, 2017.