Engineering of Science and Military Technologies
Volume (3) - Issue (1) - Mar 2019

ISSN: 2357-0954
DOI: 10.21608/ejmtc.2019.9737.1105

Extracting algebraic equations of the 2-key simplified 3-DES for algebraic cryptanalysis

Review Article

Mostafa Abdelwahab[1], Mohamed Rizk[1], Hossam Slim[2]

[1]Electrical Engineering Department, Faculty of Engineering, Alexandria University, [2]Computer Engineering Department, Faculty of Engineering and Technology, Arab Academy for Science and Technology and Maritime Transport, Alexandria, Egypt.

Keywords:
Algebraic cryptanalysis, algebraic equations, 2-key 3-DES, 2-key simplified 3-DES.

Corresponding Author:
Mostafa Abdelwahab, Electrical Engineering Department, Faculty of Engineering, Alexandria University, Alexandria, Egypt, **Tel:** 01002199625

Email: mostafa.abdelwahab@alexu.edu.eg.

Abstract
Block ciphers cryptanalysis is serious challenge specially with the existing of the powerful block ciphers that require massive number of plaintext-ciphertext pairs to perform a successful attack. Algebraic attack is superior among different attack types as it does require the smallest number of such pairs. On the other hand, the equations describe the input/output relations should be in hand to execute the algebraic attack. In this paper, we present the method of collecting the input/output algebraic equations for 2-key simplified 3-DES as a miniature example of the 2-key 3-DES. The simplified DES has similar structure and characteristics to DES with the privilege of using smaller parameters than DES. Also, we prove that the complementation property of DES can be used to double the number of obtained algebraic equations for 3-DES variants and consequently decreasing the required number of plaintext-ciphertext pairs. Finally, we compared the expected number of obtained equations and variables in both 2-key simplified 3-DES and 2-key 3-DES.

I. INTRODUCTION

The simplified DES algorithm itself is referred to as S-DES in which data are encrypted in 8-bit blocks using a 10-bit key. The decryption algorithm takes the 8-bit block of ciphertext with the same 10-bit key used in the encryption and recovers the 8-bit block of the original plaintext. As shown in figure 1, the encryption algorithm utilizes five functions[1] that are an initial permutation (IP), two complex functions (f_k) that involves permutation and substitution operations and depend on different key input for each function, a simple permutation function that swaps the two halves of the data block (SW), and finally a permutation function (IP^{-1}) which is the inverse of the first initial permutation. The decryption algorithm is the reverse of the encryption algorithm.

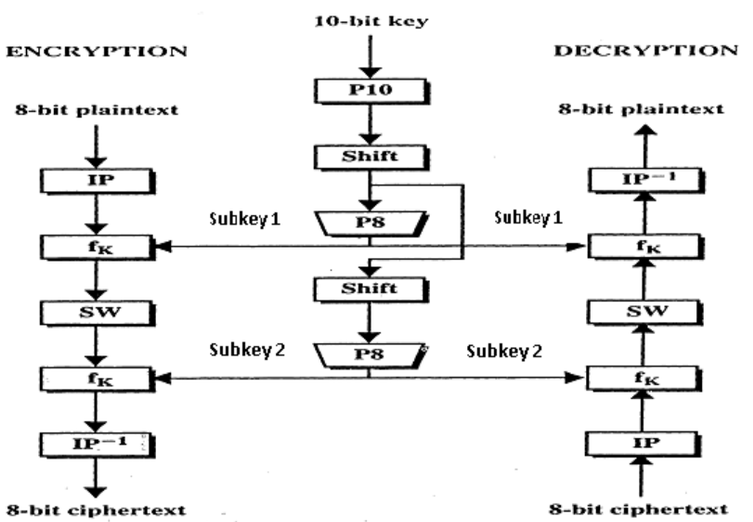

Fig. 1: Simplified DES structure

As shown in figure 2, the function f_k is the most complex and important component of the S-DES. It mixes the data passing through the encryption algorithm or the decryption algorithm with the 8-bit subkey. It involves a combination of permutations functions that represented by P4 and E/P, and substitutions functions represented by S-boxes S0 and S1.

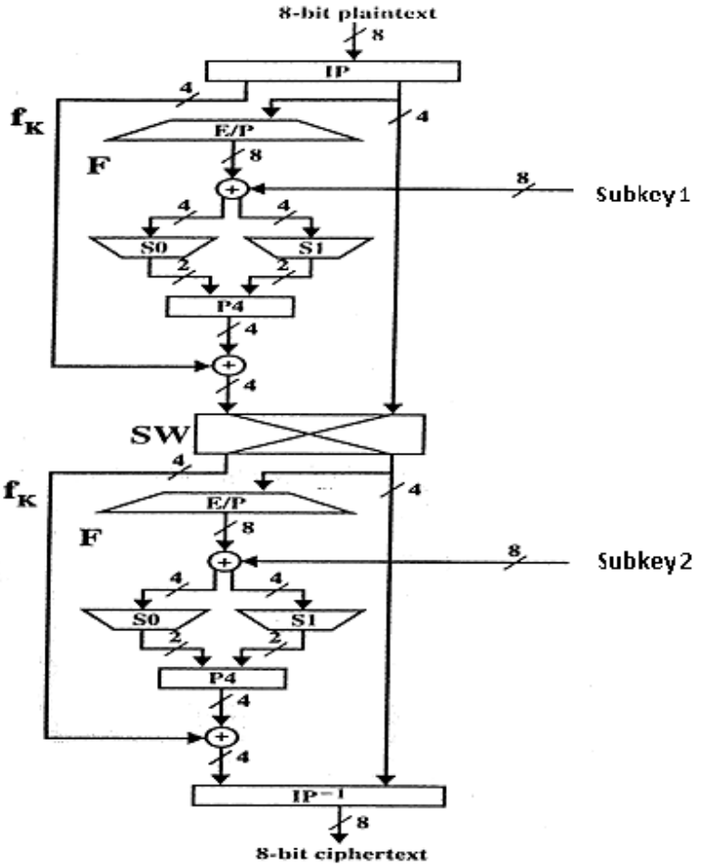

Fig. 2: Simplified DES encryption in details

The function f_k can be expressed by using equation 1 as follows:

$$f_k (L, R) = (L \oplus F(R, SK), R) \quad (1)$$

Where L and R are the leftmost 4 bits and the rightmost 4 bits of the 8-bit input to f_k respectively, SK is the used subkey, and $\oplus$ is the bit by bit XOR function. Function F is the mapping that involves expansion/permutation (E/P) of the rightmost 4 bits to produce 8 bits then bitwise XORed with the 8-bit subkey then apply substitutions using S-boxes S0, and S1 that each S-box receives 4-bit input and produce 2-bit output and finally apply permutation P4 to get a 4-bit block of data.

The expansion/permutation operation (E/P) expands and transforms a 4-bit input (i/p1, i/p 2, i/p 3, i/p 4) to 8-bit output with a particular order clarified by equation 2 as follows:

E/P (i/p 1, i/p 2, i/p 3, i/p 4) = i/p 4, i/p 1, i/p 2, i/p 3, i/p 2, i/p 3, i/p 4, and i/p 1 (2)

The S-DES has 4x2 S-boxes S0, and S1 where each S-box has 4 input bits and 2 output bits. They can be represented by the following two 4x4 matrices as shown in figure 3 where the first and last input bits to each S-box form a 2-bit number that specifies one of the four rows of the S-box . The middle two input bits specify one of the four possible columns. The permutation (P4) transforms a 4-bit input (i/p1, i/p 2, i/p 3, i/p 4) to 4-bit output with the following particular order clarified by equation 3 as follows:

P4 (i/p 1, i/p 2, i/p 3, i/p 4) = i/p 2, i/p 4, i/p 3, i/p 1 (3)

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \quad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

Fig. 3: S-boxes S0, and S1 of the S-DES [1]

The switch function (SW) swaps the left most 4 bits with the right most 4 bits before proceeding to the next round. The initial permutation (IP) transforms an 8-bit input (i/p1, i/p2, i/p3, i/p4, i/p5, i/p6, i/p7, i/p8) to 8-bit output with the following order according to equation 4 as follows:

IP (i/p1, i/p2, …, i/p8) = i/p2, i/p6, i/p3, i/p1, i/p4, i/p8, i/p5, i/p7 (4)

Whereas the inverse permutation (IP^{-1}) is the reverse of the initial permutation and can be represented by equation 5 as follows:

IP^{-1} (i/p1, i/p2, …, i/p8) = i/p4, i/p1, i/p3, i/p5, i/p7, i/p2, i/p8, i/p6. (5)

As shown in figure 4, the simplified DES uses a 10-bit key and from this key, two 8-bit subkeys (subkey 1, subkey 2) are generated to be used in the two rounds of the simplified DES, where each of the two rounds uses different subkey. As the simplified DES can be applied as encryption algorithm using the two subkey in specific order, it also can be applied as decryption algorithm using the subkeys in the reverse order. For instance, we use subkey 1 in the first round, and subkey 2 in the second round in the case of encryption, but we use subkey 2 in the first round, and subkey 1 in the second round in the case of decryption.

The 10-bit key is first introduced to permutation operation (P10) that reorder the input key bits (i/p1, i/p2, i/p3, i/p4, i/p5, i/p6, i/p7, i/p8, i/p9, i/p10) in a fashion clarified by equation 6 as follows:

P10 (i/p\1, i/p2, …, i/p10) = i/p3, i/p5, i/p2, i/p7, i/p4, i/p10, i/p1, i/p9, i/p8, i/p66. (6)

The left shift (LS-1) translates the left most bit to the right most bit position, whereas the left shift (LS-2) repeats the (LS-1) operation two consecutive times. The permutation (P8) transforms an 8-bit input (i/p1, i/p2, i/p3, i/p4, i/p5, i/p6, i/p7, i/p8) to 8-bit output with a particular order according to equation 7 as follows:

P8 (i/p1, i/p2, …, i/p8) = i/p6, i/p3, i/p7, i/p4, i/p8, i/p5, i/p10, i/p9 (7)

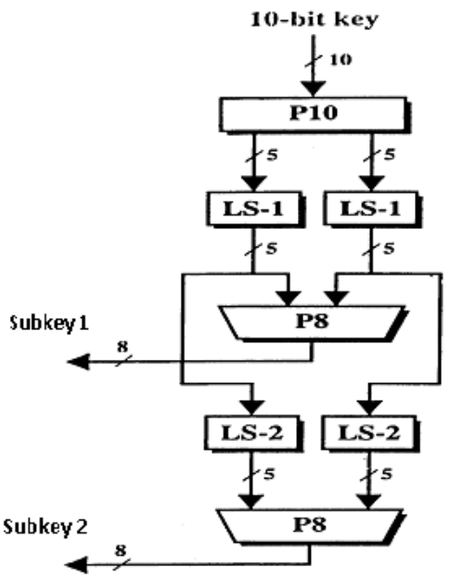

Fig. 4: Key generation of the simplified DES.

II. INPUT/OUTPUT EQUATION OF THE 2-KEY 3-SIMPLIFIED DES SCHEME

Consider the following 2-key 3-S-DES illustrated in figure 5 which involves a three stages as follows:

- Stage1: Encryption of plaintext P using key K1 to produce C1.
- Stage 2: Decryption of C1 using key K2 to produce C2.
- Stage 3: Encryption of C2 using key K1 to produce ciphertext C3.

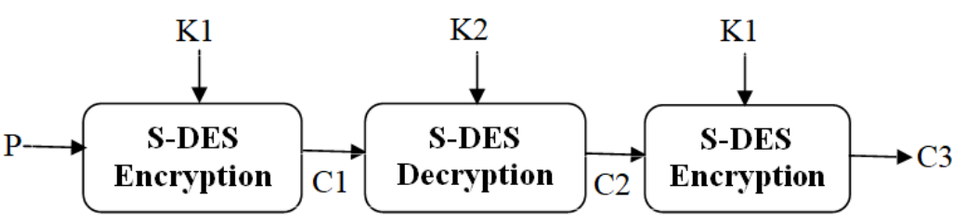

Fig. 5: 2-Key simplified 3-DES schematic diagram

Let the plaintext P = [p_1 p_2 p_3 p4 p_5 p_6 p_7 p_8], C1= [c_{11} c_{12} c_{13} c_{14} c_{15} c_{16} c_{17} c_{18}], C2= [c_{21} c_{22} c_{23} c_{24} c_{25} c_{26} c_{27} c_{28}], and C3= [c_{31} c_{32} c_{33} c_{34} c_{35} c_{36} c_{37} c_{38}].

Let K1= [k_{11} k_{12} k_{13} k_{14} k_{15} k_{16} k_{17} k_{18} k_{19} k_{110}], and K2= [k_{21} k_{22} k_{23} k_{24} k_{25} k_{26} k_{27} k_{28} k_{29} k_{210}].

Now we are going to get subkey1 and subkey2 for the three stages with the provision that subkey1, and subkey2 for the first and the third stages are identical as they derived from the same key K1.

Let subkey 1, and subkey 2 for the first and third stages are denoted by K1', and K2', respectively. Similarly, let subkey 1, and subkey 2 for the second stages are denoted by K1" and K2", respectively. The target is to get K1', K2', K1" and K2" in terms of K1 and K2. Referring to figure 4, it is clear that K1' can be expressed by using equation 8 as follows:

K1' = P8 (left and right halves LS-1 (P10 (K1))) (8)

K1' = P8 (left and right halves LS-1(P10 [k_{11} k_{12} k_{13} k14 k_{15} k_{16} k_{17} k_{18} k_{19} k_{110}]))
K1' = P8 (left and right halves LS-1 [k_{13} k_{15} k_{12} k_{17} k_{14} k_{110} k_{11} k_{19} k_{18} k_{16}])
K1' = P8 ([k_{15} k_{12} k_{17} k_{14} k_{13} k_{11} k_{19} k_{18} k_{16} k_{110}])
Hence, K1'= [k_{11} k_{17} k_{19} k_{14} k_{18} k_{13} k_{110} k_{16}]

Also, K2' can be expressed by using equation 9 as follows:

K2' = P8 (left and right halves LS-2 (LS-1 (P10 (K1)))) (9)

K2' = P8 (left and right halves LS-2 [k_{15} k_{12} k_{17} k_{14} k_{13} k_{11} k_{19} k_{18} k_{16} k_{110}])
K2' = P8 ([k_{17} k_{14} k_{13} k_{15} k_{12} k_{18} k_{16} k_{110} k_{11} k_{19}])
Hence, K2' = [k_{18} k_{13} k_{16} k_{15} k_{110} k_{12} k_{19} k_{11}]

Similarly to K1', we can calculate K1" by using equation 10 as follows:

K1" = P8 (left and right halves LS-1 (P10 (K2))) (10)

K1" = P8 (left and right halves LS-1(P10 [k_{21} k_{22} k_{23} k_{24} k_{25} k_{26} k_{27} k_{28} k_{29} k_{210}]))
K1" = P8 (left and right halves LS-1 [k_{23} k_{25} k_{22} k_{27} k_{24} k_{210} k_{21} k_{29} k_{28} k_{26}])
K1" = P8 ([k_{25} k_{22} k_{27} k_{24} k_{23} k_{21} k_{29} k_{28} k_{26} k_{210}])
Hence, K1"= [k_{21} k_{27} k_{29} k_{24} k_{28} k_{23} k_{210} k_{26}]

Similarly to K2', we can calculate K2" by using equation 11 as follows:

K2" = P8 (left and right halves LS-2 (LS-1 (P10 (K2)))) (11)

K2" = P8 (left and right halves LS-2 [k_{25} k_{22} k_{27} k_{24} k_{23} k_{21} k_{29} k_{28} k_{26} k_{210}])
K2" = P8 ([k_{27} k_{24} k_{23} k_{25} k_{22} k_{28} k_{26} k_{210} k_{21} k_{29}])
Hence, K2" = [k_{28} k_{23} k_{26} k_{25} k_{210} k_{22} k_{29} k_{21}]

We will collect the input/output equations of the first stage, then use the output of the first stage as an input to the second stage, and finally use the output of the second stage as an input to the third stage.

A. Input/output Equations of the First Stage of 2-Key 3-Simplified DES Scheme

Starting with the first stage as shown in figure 6, the plaintext P = [p_1 p_2 p_3 p_4 p_5 p_6 p_7 p_8] is introduced to IP operation to yield [p_2 p_6 p_3 p_1 p_4 p_8 p_5 p_7], then the right most 4-bit half of this data block is introduced to E/P operation to result 8-bit block that is [p_7 p_4 p_8 p_5 p_8 p_5 p_7 p_4]. That 8-bit block is XORed with K1' to result the following 8 bits which is better to write in a 2-row form as follows:

$p_7 \oplus k_{11}$ $p_4 \oplus k_{17}$ $p_8 \oplus k_{19}$ $p_5 \oplus k_{14}$
$p_8 \oplus k_{18}$ $p_5 \oplus k_{13}$ $p_7 \oplus k_{10}$ $p_4 \oplus k_{16}$

The first raw is fed to S-box S_0, whereas the second raw is fed to S-box S1. As each S-box has 4 input bits and 2 output bits, we denote the input bit to the S-box by the symbol S_{nivm} where, n refers to the n^{th} input and takes one of the four values (1, 2, 3. or 4), i refers to any input bit, v refers to S-box S0 or S1 so it takes (0 or 1), m is the round number and it takes one of the six values (1, 2, 3, 4, 5, or 6) as we have 2 rounds in each of the three stages. For example S1i01 is the first input bit of S-box S0 in round 1 which is equal to $p_7 \oplus k_{11}$. Also, we denote the output bit of the S-box by the symbol S_{wpvm} where, w refers to the w^{th} output and takes one of the two values (1, or 2), p refers to any output bit. For example S_{1p11} is the first output bit of S-box S1 in round 1.

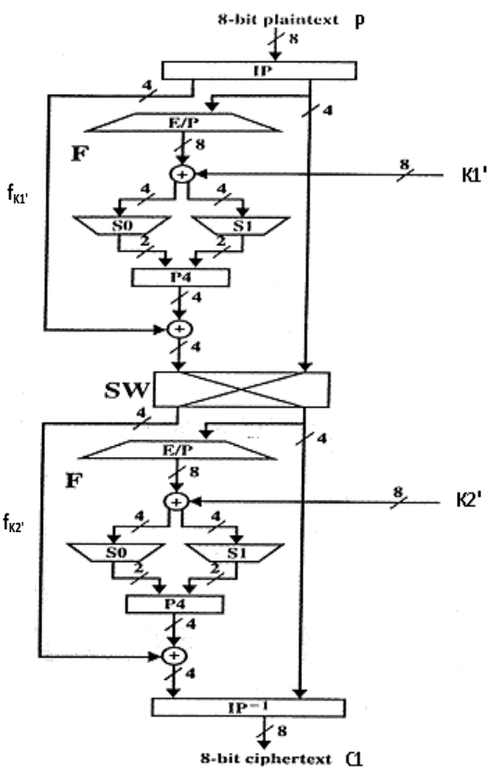

Fig. 6: The first stage of the 2-key simplified 3-DES

Now in order to proceed, we need to find the input/output two equations for each S-box. To achieve this task, we will write each S-box in the form of the truth table, and then we use the Simple Solver software[2] to transform each truth table to logical gates equation.

After applying the Simple Solver software to the truth table of S-box S0 that is illustrated in table 1, we obtain the equations 12 and 13 as follows:

$$S_{1p0m} = S_{1i0m}.S_{2i0m}.S_{4i0m} + S_{1i0m}.S_{3i0m}.S^{-}_{4i0m} + S_{1i0m}.S^{-}_{3i0m}.S_{4i0m} + S^{-}_{1i0m}.S_{2i0m}.S^{-}_{4i0m} + S^{-}_{1i0m}.S^{-}_{2i0m}.S_{4i0m} \quad (12)$$

$$S_{2p0m} = S_{1i0m}.S_{2i0m}.S^{-}_{4i0m} + S_{1i0m}.S^{-}_{2i0m}.S_{4i0m} + S^{-}_{1i0m}.S^{-}_{3i0m} + S^{-}_{3i0m}.S_{4i0m} \quad (13)$$

Where the logical operations AND, OR, and NOT are represented by symbols (.), (+), and (¯), respectively[3]. The NOT operation is also referred to the complement operation.

Table 1: The truth table of S-box S0

S_{1i0m}	S_{2i0m}	S_{3i0m}	S_{4i0m}	S_{1p0m}	S_{1p0m}
0	0	0	0	0	1
0	0	0	1	1	1
0	0	1	0	0	0
0	0	1	1	1	0
0	1	0	0	1	1
0	1	0	1	0	1
0	1	1	0	1	0
0	1	1	1	0	0
1	0	0	0	0	0
1	0	0	1	1	1
1	0	1	0	1	0
1	0	1	1	0	1
1	1	0	0	0	1
1	1	0	1	1	1
1	1	1	0	1	1
1	1	1	1	1	0

Table 2: The truth table of S-box S1

S_{1i1m}	S_{2i1m}	S_{3i1m}	S_{4i1m}	S_{1p1m}	S_{S2p1m}
0	0	0	0	0	0
0	0	0	1	1	0
0	0	1	0	0	1
0	0	1	1	0	0
0	1	0	0	1	0
0	1	0	1	0	1
0	1	1	0	1	1
0	1	1	1	1	1
1	0	0	0	1	1
1	0	0	1	1	0
1	0	1	0	0	0
1	0	1	1	0	1
1	1	0	0	0	1
1	1	0	1	0	0
1	1	1	0	0	0
1	1	1	1	1	1

Similarly, after applying the Simple Solver software to the truth table of S-box S_1 which is demonstrated in table 2, we obtain the equations 14 and 15 as follows:

$$S_{1p1m} = S_{1i1m}.\bar{S}_{2i1m}.\bar{S}_{3i1m} + S_{2i1m}.S_{3i1m}.S4i1m + \bar{S}_{1i1m}.S_{2i1m}.\bar{S}_{4i1m} + \bar{S}_{2i1m}.\bar{S}_{3i1m}.S_{4i1m} \quad (14)$$

$$S_{2p1m} = S_{1i1m}.S_{3i1m}.S_{4i1m} + S_{1i1m}.\bar{S}_{3i1m}.\bar{S}_{4i1m} + \bar{S}_{1i1m}.S_{2i1m}.S_{4i1m} + \bar{S}_{1i1m}.S_{3i1m}.\bar{S}_{4i1m} \quad (15)$$

Now, we are ready to proceed to calculate S_{1p0m}, S_{2p0m} for round 1 (m=1) by substituting in equations 12 and 13 by the following inputs:

$S_{1i01} = p_7 \oplus k_{11}$, $S_{2i01} = p_4 \oplus k_{17}$, $S_{3i01} = p_8 \oplus k_{19}$ and $S_{4i01} = p_5 \oplus k_{14}$

Then, we have calculated the two output bits for S-box S0 for round 1 that are clarified by equations 16 and 17 as follows:

$$S_{1p01} = (p_7 \oplus k_{11}).(p_4 \oplus k_{17}).(p_5 \oplus k_{14}) + (p_7 \oplus k_{11}).(p_8 \oplus k_{19})\bar{}.(p_5 \oplus k_{14})\bar{} + (p_7 \oplus k_{11})\bar{}.(p_4 \oplus k_{17}).(p_5 \oplus k_{14})\bar{} + (p_7 \oplus k_{11})\bar{}.(p_4 \oplus k_{17})\bar{}.(p_5 \oplus k_{14}) \quad (16)$$

$$S_{2p01} = (p_7 \oplus k_{11}).(p_4 \oplus k_{17}).(p_5 \oplus k_{14})\bar{} + (p_7 \oplus k_{11}).(p_4 \oplus k_{17})\bar{}.(p_5 \oplus k_{14}) + (p_7 \oplus k_{11})\bar{}.(p_8 \oplus k_{19})\bar{} + (p_8 \oplus k_{19})\bar{}.(p_5 \oplus k_{14}) \quad (17)$$

Similarly, proceed to calculate S_{1p1m} and S_{2p1m} for round 1 by substituting in equations 14 and 15 by the following inputs:

$S_{1i11} = p_8 \oplus k_{18}$, $S_{2i11} = p_5 \oplus k_{13}$, $S_{3i11} = p_7 \oplus k_{10}$, and $S_{4i11} = p_4 \oplus k_{16}$

Then, we have calculated the two output bits for S-box S_1 for round 1 that are clarified by equations 18 and 19 as follows:

$$S_{1p11} = (p_8 \oplus k_{18}).(p_5 \oplus k_{13})\bar{}.(p_7 \oplus k_{10})\bar{} + (p_5 \oplus k_{13}).(p_7 \oplus k_{10}).(p_4 \oplus k_{16}) + (p_8 \oplus k_{18})\bar{}.(p_5 \oplus k_{13}).(p_4 \oplus k_{16})\bar{} + (p_5 \oplus k_{13})\bar{}.(p_7 \oplus k_{10})\bar{}.(p_4 \oplus k_{16}) \quad (18)$$

$$S_{2p11} = (p_8 \oplus k_{18}).(p_7 \oplus k_{10}).(p_4 \oplus k_{16}) + (p_8 \oplus k_{18}).(p_7 \oplus k_{10})\bar{}.(p_4 \oplus k_{16})\bar{} + (p_8 \oplus k_{18})\bar{}.(p_5 \oplus k_{13}).(p_4 \oplus k_{16}) + (p_8 \oplus k_{18})\bar{}.(p_7 \oplus k_{10}).(p_4 \oplus k_{16})\bar{} \quad (19)$$

Now, the previously obtained four output bits from S-boxes S0 and S1 [S_{1p01} S_{2p01} S_{1p11} S_{2p11}] are fed to P4 operation to result [S_{2p01} S_{2p11} S_{1p11} S_{1p01}], then XORed with the left most 4-bit block output from IP operation to yield [$S_{2p01} \oplus p_2$ $S_{2p11} \oplus p_6$ $S_{1p11} \oplus p_3$ $S_{1p01} \oplus p_1$] which is considered the output of $f_{K1'}$ function.

The previously obtained output of $f_{K1'}$ function with the right most 4-bit block output from IP operation are fed to SW operation to yield the output 8-bit block from round 1 which is [p_4, p_8, p_5, p_7, $S_{2p01} \oplus p_2$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{1p01} \oplus p_1$]. That 8–bit block output is fed as an input to round 2 where the right most 4-bit block of that input is fed to E/P operation of $f_{K2'}$ function to yield the following 8-bit data block:

[$S_{1p01} \oplus p_1$, $S_{2p01} \oplus p_2$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{1p01} \oplus p_1$, $S_{2p01} \oplus p_2$] which is XORed with the subkey K2' = [k_{18} k_{13} k_{16} k_{15} k_{110} k_{12} k_{19} k_{11}] to yield 8 bits which is written in a 2-row form as follows:

$S_{1p01} \oplus p_1 \oplus k_{18}$, $S_{2p01} \oplus p_2 \oplus k_{13}$, $S_{2p11} \oplus p_6 \oplus k_{16}$, $S_{1p11} \oplus p_3 \oplus k_{15}$,
$S_{2p11} \oplus p_6 \oplus k_{110}$, $S_{1p11} \oplus p_3 \oplus k_{12}$, $S_{1p01} \oplus p_1 \oplus k_{19}$, $S_{2p01} \oplus p_2 \oplus k_{11}$

The first row is fed to S-box S_0, whereas the second row is fed to S-box S_1. The resultant four output bits (S_{1p02}, S_{2p02}, S_{1p12}, S_{2p12}) can be deduced by substituting for the previously mentioned 2-row input bits in the equations 12, 13, 14, and 15 taking into consideration that m = 2 to yield equations 20, 21, 22, and 23 as follows:

$$S_{1p02} = (S_{1p01} \oplus p_1 \oplus k_{18}).(S_{2p01} \oplus p_2 \oplus k_{13}).(S_{1p11} \oplus p_3 \oplus k_{15}) + (S_{1p01} \oplus p_1 \oplus k_{18}).(S_{2p11} \oplus p_6 \oplus k_{16}).(S_{1p11} \oplus p_3 k_{15})\bar{} + (S_{1p01} \oplus p_1 \oplus k_{18}).(S_{2p11} \oplus p_6 \oplus k_{16})\bar{}.(S_{1p11} \oplus p_3 \oplus k_{15}) + (S_{1p01} \oplus p_1 \oplus k_{18}).(S_{2p01} \oplus p_2 \oplus k_{13}).(S_{1p11} \oplus p_3 \oplus k_{15})\bar{} + (S_{1p01} \oplus p_1 \oplus k_{18})\bar{}.(S_{2p01} \oplus p_2 \oplus k_{13})\bar{}.(S_{1p11} \oplus p_3 \oplus k_{15}) \quad (20)$$

$$S_{2p02} = (S_{1p01} \oplus p_1 \oplus k_{18}).(S_{2p01} \oplus p_2 \oplus k_{13}).S_{1p11} \oplus p_3 \oplus k_{15})\bar{} + (S_{1p01} \oplus p_1 \oplus k_{18}).(S_{2p01} \oplus p_2 \oplus k_{13})\bar{}.(S1p11 \oplus p_3 \oplus k_{15}) + (S_{1p01} \oplus p_1 \oplus k_{18})\bar{}.(S_{2p11} \oplus p_6 \oplus k_{16})\bar{} + (S_{2p11} \oplus p_6 \oplus k_{16})\bar{}.(S_{1p11} \oplus p_3 \oplus k_{15}) \quad (21)$$

$$S_{1p12} = (S_{2p11} \oplus p_6 \oplus k_{110}).(S_{1p11} \oplus p_3 \oplus k_{12})\bar{}.(S_{1p01} \oplus p_1 \oplus k_{19})\bar{} + (S_{1p11} \oplus p_3 \oplus k_{12}).(S_{1p01} \oplus p_1 \oplus k_{19}).(S_{2p01} \oplus p_2 \oplus k_{11}) + (S_{2p11} \oplus p_6 \oplus k_{110})\bar{}.(S_{1p11} \oplus p_3 \oplus k_{12}).(S_{2p01} \oplus p_2 \oplus k_{11})\bar{} + (S_{1p11} \oplus p_3 \oplus k_{12})\bar{}.(S_{1p01} \oplus p_1 \oplus k_{19})\bar{}.(S_{2p01} \oplus p_2 \oplus k_{11}) \quad (22)$$

$$S_{2p12} = (S_{2p11} \oplus p_6 \oplus k_{110}).(S_{1p01} \oplus p_1 \oplus k_{19}).(S_{2p01} \oplus p_2 \oplus k_{11}) + (S_{2p11} \oplus p_6 \oplus k_{110}).(S_{1p01} \oplus p_1 \oplus k_{19})\bar{}.(S_{2p01} \oplus p_2 \oplus k11)\bar{} + (S_{2p11} \oplus p_6 \oplus k_{110})\bar{}.(S_{1p11} \oplus p_3 \oplus k_{12}).(S_{2p01} \oplus p_2 \oplus k_{11}) + (S_{2p11} \oplus p_6 \oplus k_{110})\bar{}.(S_{1p01} \oplus p_1 \oplus k_{19}).(S_{2p01} \oplus p_2 \oplus k_{11})\bar{} \quad (23)$$

The previously obtained 4-bit output from S-boxes S0 and S1 is [S_{1p02}, S_{2p02}, S_{1p12}, S_{2p12}] that is introduced to P4 operation to result [S_{2p02} S_{2p12} S_{1p12} S_{1p02}] then XORed with the left most 4-bit output from SW operation to yield [$S_{2p02} \oplus p_4$, $S_{2p12} \oplus p_8$, $S_{1p12} \oplus p_5$, $S_{1p02} \oplus p_7$] which is considered the output block of $f_{K2'}$ function. Then the obtained 8-bit data block [$S_{2p02} \oplus p_4$, $S_{2p12} \oplus p_8$, $S_{1p12} \oplus p_5$, $S_{1p02} \oplus p_7$, $S_{2p01} \oplus p_2$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{1p01} \oplus p_1$] is fed to IP^{-1} operation to result C1 = [$S_{1p02} \oplus p_7$, $S_{2p02} \oplus p_4$, $S_{1p12} \oplus p_5$, $S_{2p01} \oplus p_2$, $S_{1p11} \oplus p_3$, $S_{2p12} \oplus p_8$, $S_{1p01} \oplus p_1$, $S_{2p11} \oplus p_6$] that is considered the output 8-bit block from the first stage.

B. Input/output Equations of the Second Stage of 2-Key 3-Simplified DES Scheme

The previously obtained output from the first stage C1 = [$S_{1p02} \oplus p_7$, $S_{2p02} \oplus p_4$, $S_{1p12} \oplus p_5$, $S_{2p01} \oplus p_2$, $S_{1p11} \oplus p_3$, $S_{2p12} \oplus p_8$, $S_{1p01} \oplus p_1$, $S_{2p11} \oplus p_6$] is fed as an input to the second stage of the 2-key simplified 3-DES as shown in figure 7.

Then, C1 is introduced to IP operation to yield [$S_{2p02} \oplus p_4$, $S_{2p12} \oplus p_8$, $S_{1p12} \oplus p_5$, $S_{1p02} \oplus p_7$, $S_{2p01} \oplus p_2$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{1p01} \oplus p_1$], then the right most 4-bit half of this data block is introduced to E/P operation to result 8-bit block that is [$S_{1p01} \oplus p_1$, $S_{2p01} \oplus p_2$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{1p01} \oplus p_1$, $S_{2p01} \oplus p_2$]. That 8-bit block is XORed with K2" to result the following 8 bits which is better to write in a 2-row form as follows:

$S_{1p01} \oplus p_1 \oplus k_{28}$ $S_{2p01} \oplus p_2 \oplus k_{23}$ $S_{2p11} \oplus p_6 \oplus k_{26}$ $S_{1p11} \oplus p_3 \oplus k_{25}$

$S_{2p11} \oplus p_6 \oplus k_{210}$ $S_{1p11} \oplus p_3 \oplus k_{22}$ $S_{1p01} \oplus p_1 \oplus k_{29}$ $S_{2p01} \oplus p_2 \oplus k_{21}$

The first row is fed to S-box S0, whereas the second row is fed to S-box S1. Now we are ready to proceed to calculate S_{1p0m}, S_{2p0m} for round 3 (m=3) by substituting in equations 12 and 13 by the following inputs:
$S_{1i03} = S_{1p01} \oplus p_1 \oplus k_{28}$, $S_{2i03} = S_{2p01} \oplus p_2 \oplus k_{23}$, $S_{3i03} = S_{2p11} \oplus p_6 \oplus k_{26}$, $S_{4i03} = S_{1p11} \oplus p_3 \oplus k_{25}$

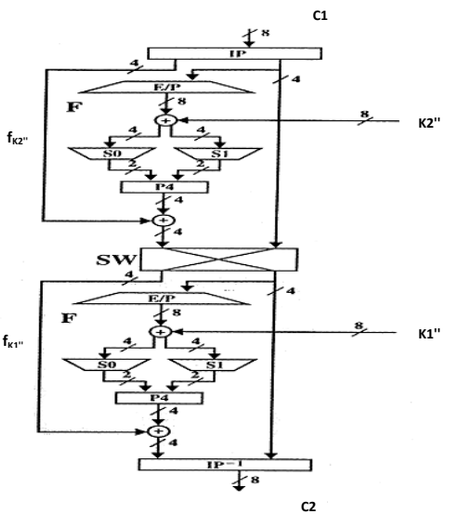

Fig. 7: The second stage of the 2-key simplified 3-DES

Then, we have calculated the two output bits for S-box S0 for round 3 that are clarified by equations 24 and 25 as follows:

$$S_{1p03} = (S_{1p01} \oplus p_1 \oplus k_{28}).(S_{2p01} \oplus p_2 \oplus k_{23}).(S_{1p11} \oplus p_3 \oplus k_{25}) + (S_{1p01} \oplus p_1 \oplus k_{28}).(S_{2p11} \oplus p_6 \oplus k_{26}).(S_{1p11} \oplus p_3 \oplus k_{25})^- + (S_{1p01} \oplus p_1 \oplus k_{28}).(S_{2p11} \oplus p_6 \oplus k_{26})^-.(S_{1p11} \oplus p_3 \oplus k_{25}) + (S_{1p01} \oplus p_1 \oplus k_{28})^-.(S_{2p01} \oplus p_2 \oplus k_{23}).(S_{1p11} \oplus p_3 \oplus k_{25})^- + (S_{1p01} \oplus p_1 \oplus k_{28})^-.(S_{2p01} \oplus p_2 \oplus k_{23})^-.(S_{1p11} \oplus p_3 \oplus k_{25}) \quad (24)$$

$$S_{2p03}=(S_{1p01} \oplus p_1 \oplus k_{28}).(S_{2p01} \oplus p_2 \oplus k_{23}).(S_{1p11} \oplus p_3 \oplus k_{25})^- + (S_{1p01} \oplus p_1 \oplus k_{28}).(S_{2p01} \oplus p_2 \oplus k_{23})^-.(S_{1p11} \oplus p_3 \oplus k_{25}) + (S_{1p01} \oplus p_1 \oplus k_{28})^-.(S_{2p11} \oplus p_6 \oplus k_{26})^- + (S_{2p11} \oplus p_6 \oplus k_{26})^-.(S_{1p11} \oplus p_3 \oplus k_{25}) \quad (25)$$

Similarly, proceed to calculate S_{1p13} and S_{2p13} for round 3 by substituting in equations 14 and 15 by the following inputs:
$S_{1i13} = S_{2p11} \oplus p_6 \oplus k_{210}$, $S_{2i13} = S_{1p11} \oplus p_3 \oplus k_{22}$, $S_{3i13} = S_{1p01} \oplus p_1 \oplus k_{29}$, $S_{4i13} = S_{2p01} \oplus p_2 \oplus k_{21}$.

Then, we have calculated the two output bits for S-box S1 for round 3 that are clarified by equations 26 and 27 as follows:

$$S_{1p13} = (S_{2p11} \oplus p_6 \oplus k_{210}).(S_{1p11} \oplus p_3 \oplus k_{22})^-.(S_{1p01} \oplus p_1 \oplus k_{29})^- + (S_{1p11} \oplus p_3 \oplus k_{22}).(S_{1p01} \oplus p_1 \oplus k_{29}) .(S_{2p01} \oplus p_2 \oplus k_{21}) + (S_{2p11} \oplus p_6 \oplus k_{210})^-.(S_{1p11} \oplus p_3 \oplus k_{22}).(S_{2p01} \oplus p_2 \oplus k_{21})^- + (S_{1p11} \oplus p_3 \oplus k_{22})^-.(S_{1p01} \oplus p_1 \oplus k_{29})^-.(S_{2p01} \oplus p_2 \oplus k_{21}) \quad (26)$$

$$S_{2p13} = (S_{2p11} \oplus p_6 \oplus k_{210}).(S_{1p01} \oplus p_1 \oplus k_{29}).(S_{2p01} \oplus p_2 \oplus k_{21}) + (S_{2p11} \oplus p_6 \oplus k_{210}).(S_{1p01} \oplus p_1 \oplus k_{29})^-.(S_{2p01} \oplus p_2 \oplus k_{21})^- + (S_{2p11} \oplus p_6 \oplus k_{210})^-.(S_{1p11} \oplus p_3 \oplus k_{22}).(S_{2p01} \oplus p_2 \oplus k_{21}) + (S_{2p11} \oplus p_6 \oplus k_{210})^-.(S_{1p01} \oplus p_1 \oplus k_{29}). (S_{2p01} \oplus p_2 \oplus k_{21})^- \quad (27)$$

The previously obtained 4-bit output from S-boxes S0 and S1 is [S_{1p03}, S_{2p03}, S_{1p13}, S_{2p13}] that is introduced to P4 operation to result [S_{2p03} S_{2p13} S_{1p13} S_{1p03}], then XORed with the left most 4-bit output from IP operation to yield [$S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$] which is considered the output block of $f_{K2"}$ function. The obtained 8-bit block [$S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$, $S_{2p01} \oplus p_2$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{1p01} \oplus p_1$] is fed to SW operation to result the 8-bit block [$S_{2p01} \oplus p_2$, $S_{2p11} \oplus p_6$, $S_{1p11} \oplus p_3$, $S_{1p01} \oplus p_1$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$] that is considered the output 8-bit block from the round 3. That 8–bit output block is fed as an input to round 4 where the right most 4-bit block of that input is fed to E/P operation of fK1" function to yield the following 8-bit data block:

[$S_{1p02} \oplus p_7 \oplus S_{1p03}$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$], which is XORed with the subkey K1" to yield 8 bits which is written in a 2-row form as follows:

$S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21}$, $S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{27}$, $S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{29}$, $S1p12 \oplus p_5 \oplus S_{1p13} \oplus k_{24}$,
$S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{28}$, $S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{23}$, $S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{210}$, $S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{26}$

The first row is fed to S-box S0, whereas the second row is fed to S-box S1. The resultant four output bits (S_{1p04}, S_{2p04}, S_{1p14}, S_{2p14}) can be deduced by substituting for the previously mentioned 2-row input bits in the equations 12, 13, 14, and 15 taking into consideration that m = 4 to yield equations 28, 29, 30, and 31 as follows:

$$S_{1p04} = (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21}).(S2p02 \oplus p4 \oplus S_{2p03} \oplus k_{27}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{24}) + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21}).(S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{29}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{24})^- + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21}).(S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{29})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{24}) + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{27}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{24})^- + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21})^-.(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{27})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{24}) \quad (28)$$

$$S_{2p04} = (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{27}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{24})^- + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{27})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{24}) + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{21})^-.(S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k29)^- + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{29})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{24}) \quad (29)$$

$$S_{1p14} = (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{28}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{23})^-.(S_{1p02} \oplus p_7 S_{1p03} \oplus k_{210})^- + (S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{23}).(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{210}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{26}) + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{28})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{23}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{26})^- + (S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{23})^-.(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{210})^-.(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{26}) \quad (30)$$

$$S_{2p14} = (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{28}).(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{210}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{26}) + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{28}).(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{210})^-.(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{26})^- + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{28})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{23}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{26}) + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{28}).(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{210}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{26})^- \quad (31)$$

The previously obtained 4-bit output from S-boxes S_0 and S_1 is [S_{1p04}, S_{2p04}, S_{1p14}, S_{2p14}] that is introduced to P4 operation to result [S_{2p04} S_{2p14} S_{1p14} S_{1p04}], then XORed with the left most 4-bit output from SW operation to yield [$S_{2p01} \oplus p_2 \oplus S_{2p04}$, $S_{2p11} \oplus p_6 \oplus S_{2p14}$, $S_{1p11} \oplus p_3 \oplus S_{1p14}$, $S_{1p01} \oplus p_1 \oplus S_{1p04}$] which is considered the output block of fK1" function. Then, the obtained 8-bit data block [$S_{2p01} \oplus p_2 \oplus S_{2p04}$, $S_{2p11} \oplus p_6 \oplus S_{2p14}$, $S_{1p11} \oplus p_3 \oplus S_{1p14}$, $S_{1p01} \oplus p_1 \oplus S_{1p04}$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$] is fed to IP-1 operation to result C2 = [$S_{1p01} \oplus p_1 \oplus S_{1p04}$, $S_{2p01} \oplus p_2 \oplus S_{2p04}$, $S_{1p11} \oplus p_3 \oplus S_{1p14}$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{2p11} \oplus p_6 \oplus S_{2p14}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$] that is considered the output 8-bit block from the second stage (S-DES decryption).

C. Input/output Equations of the Third Stage of 2-Key 3-Simplified DES Scheme

The previously obtained output from the second stage C2 = [$S_{1p01} \oplus p_1 \oplus S_{1p04}$, $S_{2p01} \oplus p_2 \oplus S_{2p04}$, $S_{1p11} \oplus p_3 \oplus S_{1p14}$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{2p11} \oplus p_6 \oplus S_{2p14}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$] is fed as an input to the third stage of the 2-key simplified 3-DES as shown in figure 8. Then C2 is introduced to IP operation to yield [$S_{2p01} \oplus p_2 \oplus S_{2p04}$, $S_{2p11} \oplus p_6 \oplus S_{2p14}$, $S_{1p11} \oplus p_3 \oplus S_{1p14}$, $S_{1p01} \oplus p_1 \oplus S_{1p04}$, $S_{2p02} \oplus p4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$], then the right most 4-bit half of this data block is introduced to E/P operation to result 8-bit block that is [$S_{1p02} \oplus p_7 \oplus S_{1p03}$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$]. That 8-bit block is XORed with K1' to result the following 8 bits which is better to write in a 2-row form as follows:

$S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11}$, $S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{17}$, $S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{19}$, $S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14}$,
$S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{18}$, $S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{110}$, $S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{16}$

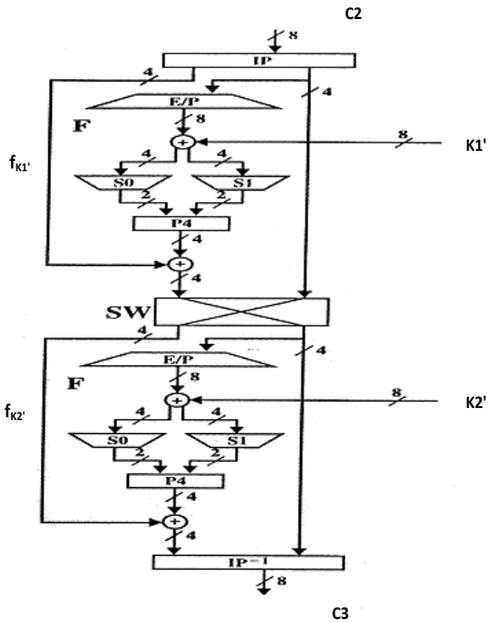

Fig. 8: The third stage of the 2-key simplified 3-DES

The first row is fed to S-box S_0, whereas the second row is fed to S-box S1. The resultant four output bits (S_{1p05}, S_{2p05}, S_{1p15}, S_{2p15}) can be derived by substituting for the previously mentioned 2-row input bits in the equations 12, 13, 14, and 15 taking into consideration that m = 5 to yield equations 32, 33, 34, and 35 as follows:

$$S_{1p05} = (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{17}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14}) + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11}).(S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{19}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14})^- + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11}).(S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{19})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14}) + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11})^-.(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{17}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14})^- + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11})^-.(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{17})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14}) \quad (32)$$

$$S_{2p05} = (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{17}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14})^- + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{17})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14}) + (S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{11})^-.(S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{19})^- + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{19})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{14}). \quad (33)$$

$$S_{1p15} = (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{18}).(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{13})^-.(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{110})^- + (S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{13}).(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{110}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{16}) + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{18})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{13}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{16})^- + (S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{13})^-.(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{110})^-.(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{16}) \quad (34)$$

$$S_{2p15} = (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{18}).(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{110}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{16}) + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{18}).(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{110})^-.(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{16})^- + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{18})^-.(S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus k_{13}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{16}) + (S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus k_{18})^-.(S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus k_{110}).(S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus k_{16})^- \quad (35)$$

The previously obtained 4-bit output from S-boxes S0 and S1 is [S_{1p05}, S_{2p05}, S_{1p15}, S_{2p15}] that is introduced to P4 operation to result [S_{2p05} S_{2p15} S_{1p15} S_{1p05}] then XORed with the left most 4-bit output data block from IP operation to result [$S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05}$, $S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15}$, $S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15}$, $S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05}$] that is considered the output block of $f_{K1'}$ function. Then the obtained 8-bit data block [$S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05}$, $S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15}$, $S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15}$, $S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05}$, $S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$] is fed to SW operation to yield the 8-bit data block as follows:

[$S_{2p02} \oplus p_4 \oplus S_{2p03}$, $S_{2p12} \oplus p_8 \oplus S_{2p13}$, $S_{1p12} \oplus p_5 \oplus S_{1p13}$, $S_{1p02} \oplus p_7 \oplus S_{1p03}$, $S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05}$, $S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15}$, $S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15}$, $S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05}$] that can be considered the output 8-bit block from round 5. That 8–bit output block is fed as an input to round 6 where the right most 4-bit block of that input is fed to E/P operation of $f_{K2'}$ function to yield the following 8-bit data block:

[$S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05}$, $S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05}$, $S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15}$, $S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15}$, $S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15}$, $S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15}$, $S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05}$, $S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05}$] which is XORed with the subkey K2' to yield 8 input bits to S-boxes S0, and S1 as follows:

$$S_{1i06} = S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18},\ S_{2i06} = S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{13},$$
$$S_{3i06} = S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{16},\ S_{4i06} = S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15},$$
$$S_{1i16} = S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{110},\ S_{2i16} = S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{12},$$
$$S_{3i16} = S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{19},\ \text{and}\ S_{4i16} = S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{11}$$

The first 4-input bits are fed to S-box S0, whereas the second 4-input bits are fed to S-box S1. The resultant four output bits (S_{1p06}, S_{2p06}, S_{1p16}, S_{2p16}) can be deduced by substituting for the previously input bits in the equations 12, 13, 14, and 15 taking into consideration that m = 6 to yield equations 36, 37, 38, and 39 as follows:

$S_{1p06} = (S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18}).(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{13}).(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15}) + (S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18}).(S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{16}).(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15})^- + (S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18}).(S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{16})^-.(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15}) + (S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18})^-.(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{13}).(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15})^- + (S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18})^-.(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{13})^-.(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15})$ (36)

$S_{2p06} = (S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18}).(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k13).(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15})^- + (S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18}).(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{13})^-.(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15}) + (S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{18})^-.(S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{16})^- + (S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{16})^-.(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{15})$ (37)

$S_{1p16} = (S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{110}).(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{12})^-.(S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{19})^- + (S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{12}).(S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{19}).(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{11}) + (S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{110})^-.(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{12}).(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{11})^- + (S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{12})^-.(S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{19})^-.(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{11})$ (38)

$S_{2p16} = (S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{110}).(S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{19}).(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{11}) + (S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{110}).(S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{19})^-.(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{11})^- + (S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{110})^-.(S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \oplus k_{12}).(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{11}) + (S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \oplus k_{110})^-.(S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \oplus k_{19}).(S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \oplus k_{11})^-$ (39)

The previously obtained 4-bit output from S-boxes S_0 and S1 is $[S_{1p06}, S_{2p06}, S_{1p16}, S_{2p16}]$ that is introduced to P4 operation to result $[S_{2p06}, S_{2p16}, S_{1p16}, S_{1p06}]$, then XORed with the left most 4-bit output from SW operation to yield $[S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus S_{2p06}, S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus S_{2p16}, S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus S_{1p16}, S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus S_{1p06}]$ which is considered the output block of $f_{K2'}$ function. Then, the obtained 8-bit data block $[S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus S_{2p06}, S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus S_{2p16}, S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus S_{1p16}, S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus S_{1p06}, S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05}, S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15}, S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15}, S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05}]$ is fed to IP^{-1} operation to result $C3 = [S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus S_{1p06}, S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus S_{2p06}, S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus S_{1p16}, S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05}, S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15}, S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus S_{2p16}, S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05}, S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15}]$ that is considered the output 8-bit block from the third stage and subsequently the output of the 2-key 3-S-DES. Hence, Boolean equations 40, 41, 42, 43, 44, 45, 46 and 47 that are guided by Boolean algebra properties and operations[4] represent the eight input/output equations of the 2-key 3-S-DES as follows:

$$c31 = S_{1p02} \oplus p_7 \oplus S_{1p03} \oplus S_{1p06} \quad (40)$$

$$c32 = S_{2p02} \oplus p_4 \oplus S_{2p03} \oplus S_{2p06} \quad (41)$$

$$c33 = S_{1p12} \oplus p_5 \oplus S_{1p13} \oplus S_{1p16} \quad (42)$$

$$c34 = S_{2p01} \oplus p_2 \oplus S_{2p04} \oplus S_{2p05} \quad (43)$$

$$c35 = S_{1p11} \oplus p_3 \oplus S_{1p14} \oplus S_{1p15} \quad (44)$$

$$c36 = S_{2p12} \oplus p_8 \oplus S_{2p13} \oplus S_{2p16} \quad (45)$$

$$c37 = S_{1p01} \oplus p_1 \oplus S_{1p04} \oplus S_{1p05} \quad (46)$$

$$c38 = S_{2p11} \oplus p_6 \oplus S_{2p14} \oplus S_{2p15} \quad (47)$$

At this point, for only one known plaintext-ciphertext it seems that we have 8 equations (40, 41,…, and 47) in 20 unknowns which are 10 bits of K1, and 10 bits of K2. It is more reasonable to solve an overdefined system of equations [5], and [6] as the complexity decreases when the number of equations exceeds the number of unknowns. This system is also known as overdetermined system of equations [7]. To construct an overdefined system of 32 equations in 20 unknowns, we need four known plaintext-ciphertext pairs. Anyway we still have the opportunity to collect more equations by exploiting the complementation property for DES as will be clarified next section.

III. EXPLOITING COMPLEMENTATION PROPERTY FOR DUPLICATING ALGEBRAIC EQUATIONS

The complementation property for DES [8] declares that, for any 64-bit block P and any DES key K, equation 48 exists as follows:

$$E_{K^-}(P^-) = (E_K(P))^- \quad (48)$$

Where, P^- represents the bit-wise complement of bit string P, K^- represents the bit-wise complement of bit string K, and $(E_K(P))^-$ represents the bit-wise complement of bit string $E_K(P)$. That means if plaintext (P) and key (K) are complemented, subsequently the ciphertext $E_K(P)$ is also complemented.

A. The Complementation Property for the 2-Key Simplified 3-DES

It is quite simple to prove that the complementation property for DES is also valid for 3-DES variants

which are 2-key 3-DES and 3-key 3-DES as follows: Consider Figure 9 which illustrates the three stages of the 3-key 3-DES where it is clear that $C = E_{K3}(D_{K2}(E_{K1}(P)))$.

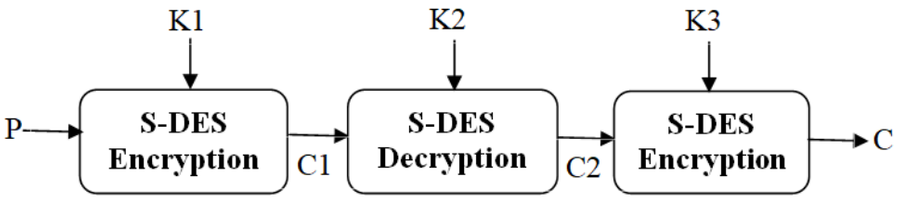

Fig. 9: Encryption of P using 2-key simplified 3-DES to produce C

Our task to prove that: $C^- = E_{K3^-}(D_{K2^-}(E_{K1^-}(P^-)))$.

According to Figure 9 and for the first stage equation 49 is correct.

$C1 = E_{k1}(P)$

Now apply the complementation property to equation 49 yields equation 50 as follows:

$$C1^- = E_{K1^-}(P^-) \quad (50)$$

Equation 51 is driven form the second stage of the 3-key 3-DES algorithm demonstrated in Figure 9.

$$C2 = D_{K2}(C1) \quad (51)$$

As DES decryption uses the same algorithm as encryption with reversed sub-keys[12], therefore the complementation property can be applied to equation 51 and yields equation 52 as follows:

$$C2^- = D_{K2^-}(C1^-) \quad (52)$$

Similarly, by applying complementation property for the third stage, it yields equation 53 as shown below:

$$C^- = E_{K3^-}(C2^-) \quad (53)$$

Now substitute for $C2^-$ from equation 52 in equation 53 results equation 54 as follows:

$$C^- = E_{K3^-}(D_{K2^-}(C1^-)) \quad (54)$$

Equation 55 can be driven by substituting for $C1^-$ from equation 50 in equation 54 as follows:

$$C^- = E_{K3^-}(D_{K2^-}(E_{K1^-}(P^-))) \quad (55)$$

According to equation 55, the complementation property is valid for 3-key triple DES.

Returning to figure 9, if we replace key K3 in the third stage by K1, we will get a 2-key 3-DES scheme with overall input/output relation $C = E_{K1}(D_{K2}(E_{K1}(P)))$.

Now to check the validity of complementation property for the 2-key 3-DES scheme, we replace K3 by K1 in equation 55, to yield equation 56 as follows:

$$C^- = E_{K1^-}(D_{K2^-}(E_{K1^-}(P^-))) \quad (56)$$

Which proves that the complementation property is also valid for the 2-key 3-DES, therefore we can exploit this property to duplicate the input/output previously obtained equations (40, 41,…, and 47) for the 2-Key Simplified 3-DES as will be done in the next subsection.

B. Collecting the Algebraic Equations Resulting from Complementation Property

Now, we are going to exploit the previously discussed complementation property by replacing $C3 = [c_{31}\ c_{32}\ c_{33}\ c34\ c_{35}\ c_{36}\ c_{37}\ c_{38}]$ by $C3^- = [c_{31}^-\ c_{32}^-\ c_{33}^-\ c_{34}^-\ c_{35}^-\ c_{36}^-\ c_{37}^-\ c_{38}^-]$, replacing $K1 = [k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{110}]$ by $K1^- = [k_{11}^-\ k_{12}^-\ k_{13}^-\ k_{14}^-\ k_{15}^-\ k_{16}^-\ k_{17}^-\ k_{18}^-\ k_{19}^-\ k_{110}^-]$, replacing $K2 = [k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{210}]$ by $K2^- = [k_{21}^-\ k_{22}^-\ k_{23}^-\ k_{24}^-\ k_{25}^-\ k_{26}^-\ k_{27}^-\ k_{28}^-\ k_{29}^-\ k_{210}^-]$, and replacing $P = [p_1\ p_2\ p_3\ p_4\ p_5\ p_6\ p_7\ p_8]$ by $P^- = [p_1^-\ p_2^-\ p_3^-\ p_4^-\ p_5^-\ p_6^-\ p_7^-\ p_8^-]$ Where, $C3^-$ represents the bit-wise complement of bit string C3, P^- represents the bit-wise complement of bit string P, $K1^-$ represents the bit-wise complement of bit string K1, and $K2^-$ represents the bit-wise complement of bit string K2. After executing the necessary replacement in the related equations to equations 40, 41, 42, 43, 44, 45, 46 and 47, we can get another eight equations that are equations 57, 58, 59, 60, 61, 62, 63 and 64 as follows:

$$c_{31}^- = S_{1p^-02} \oplus p_7^- \oplus S_{1p^-03} \oplus S_{1p^-06} \quad (57)$$

$$c_{32}^- = S_{2p^-02} \oplus p_4^- \oplus S_{2p^-03} \oplus S_{2p^-06} \quad (58)$$

$$c_{33}^- = S_{1p^-12} \oplus p_5^- \oplus S_{1p^-13} \oplus S_{1p^-16} \quad (59)$$

$$c_{34}^- = S_{2p^-01} \oplus p_2^- \oplus S_{2p^-04} \oplus S_{2p^-05} \quad (60)$$

$$c_{35}^- = S_{1p^-11} \oplus p_3^- \oplus S_{1p^-14} \oplus S_{1p^-15} \quad (61)$$

$$c_{36}^- = S_{2p^-12} \oplus p_8^- \oplus S_{2p^-13} \oplus S_{2p^-16} \quad (62)$$

$$c_{37}^- = S_{1p^-01} \oplus p_1^- \oplus S_{1p^-04} \oplus S_{1p^-05} \quad (63)$$

$$c_{38}^- = S_{2p^-11} \oplus p_6^- \oplus S_{2p^-14} \oplus S_{2p^-15} \quad (64)$$

Where the bits S_{1p^-01}, S_{2p^-01}, S_{1p^-11}, S_{2p^-11}, S_{1p^-02}, S_{2p^-02}, S_{1p^-12}, S_{2p^-12}, S_{1p^-03}, S_{2p^-03}, S_{1p^-13}, S_{2p^-13}, S_{1p^-04}, S_{2p^-04}, S_{1p^-14}, S_{2p^-14}, S_{1p^-05}, S_{2p^-05}, S_{1p^-15}, S_{2p^-15}, S_{1p^-06}, S_{2p^-06}, S_{1p^-16}, and S_{2p^-16} are obtained from the bits S_{1p01}, S_{2p01}, S_{1p11}, S_{2p11}, S_{1p02}, S_{2p02}, S_{1p12}, S_{2p12}, S_{1p03}, S_{2p03}, S_{1p13}, S_{2p13}, S_{1p04}, S_{2p04}, S_{1p14}, S_{2p14}, S_{1p05}, S_{2p05}, S_{1p15}, S_{2p15}, S_{1p06}, S_{2p06}, S_{1p16}, and S_{2p16} respectively by the necessary replacements of P, K1, and K2 by P^-, $K1^-$, and $K2^-$ respectively in the related equations .

So far it looks like that we have a system of 16 nonlinear multivariate equations (40, 41,…, and 47) and (57, 58,…, and 64) in 20 unknowns which are 10 bits of K1, 10 bits of K2 for only one known plaintext-ciphertext pair. Consequently if we have at least 2 known plaintext-ciphertext pairs, we would be able to get at least a system

of 32 nonlinear multivariate equations in 20 unknowns. This system of equation can be solved by using XLBA algorithm[9]. While as previously shown without applying complementation property, we need 4 plaintext-ciphertext pairs to collect also 32 equations in 20 unknowns, it is obvious that applying complementation property reduces the required number of plaintext-ciphertext pairs significantly by half. Therefore this property is useful as it facilitates solving such system.

IV. EXPECTED EQUATIONS FOR 2-KEY 3-DES COMPARED WITH 2-KEY SIMPLIFIED 3-DES

As we previously mentioned the simplified DES algorithm encrypt and decrypt the data in 8-bit blocks using a 10-bit key whereas the DES algorithm uses 64-bit key to encrypt or decrypt a 64-bit blocks of data. For the 2-key 3-DES we can obtain 64 equations in 128 unknowns which are 64-bit of key K1 and 64-bit of key K2. Besides extra 64 equations by exploiting the complementation property that yields an overall 128 equations in 128 unknowns for one plaintext-ciphertext pair. With two plaintext-ciphertext pairs, we would be able to get a system of 256 nonlinear multivariate equations in 128 variables for 2-key 3-DES.

Unlike many attacks such as linear and differential cryptanalysis[10], the algebraic attack does not require large number of plaintext-ciphertext pairs[11]. Moreover, the attractive feature of the algebraic attack is the ability to work as a ciphertext only attack. For the 2-key 3-DES as an example the scenario will be as follows:

1) By applying complementation property, we collect 128 equations in 192 unknowns which are 64-bit of plaintext P1, 64-bit of key K1 and 64-bit of key K2 for the first ciphertext.

2) By applying complementation property, we collect extra 128 equations in extra 64 unknowns which are 64-bit of plaintext P2, for the second ciphertext under the condition that key K1 and K2 are not changed.

3) By applying complementation property, we collect extra 128 equations in extra 64 unknowns which are 64-bit of plaintext P3, for the third ciphertext under the condition that key K1 and K2 are not changed.

It is worth pointing out that the resultant equations from step 1 and 2 are 256 equations in 256 unknowns which are 64-bit of plaintext P1, 64-bit of plaintext P2, 64-bit of key K1 and 64-bit of key K2 while the resultant equations from steps 1, 2, and 3 are 384 equations in 320 unknowns which are 64-bit of plaintext P1, 64-bit of plaintext P2, 64-bit of plaintext P3, 64-bit of key K1 and 64-bit of key K2. Therefore we can obtain overdefined system of 384 equations in 320 unknowns by utilizing the available data from 3 ciphertexts under the condition that the used keys K1 and K2 are not changed during collecting these 3 ciphertexts data. Algebraic cryptanalysis is also important during cipher design[12] because it is not only used as tool for key recovery, but also for detecting weaknesses.

V. CONCLUSIONS

In this paper, we demonstrate the method to collect the system of nonlinear multivariate Boolean algebraic equations for the 2-Key simplified 3-DES encryption system as an illustrative example of a miniature system similar to 2-Key 3-DES. We prove the validity of complementation property for 3-DES variants as well as for DES. We exploit this property to duplicate the number of obtained algebraic equations and therefore decrease the required number of plaintext-ciphertext pairs to collect an overdefined system of equations. In addition, we already get a system of 16 nonlinear multivariate equations in 20 unknowns for only one plaintext-ciphertext pair for 2-Key simplified 3-DES, consequently using only 2 plaintext-ciphertext are enough to get an overdefined system of 32 nonlinear multivariate equations in 20 unknowns. Also we compare between 2-Key 3-DES and 2-Key simplified 3-DES to estimate the expected number of obtained equations and variables for 2-Key 3-DES. We found that only 2 plaintext-ciphertext pairs are enough to get an overdefined system of 256 nonlinear multivariate equations in 128 unknowns. Finally, we show that the method of collecting algebraic equation is powerful as it gives the ability to algebraic attack to work as ciphertext only attack.

VI. ACKNOWLEDGMENT

First, thanks god for completing this paper. Secondly, the authors would like to thank Mr. Ahmed Hossam for his valuable help.

VII. REFERENCES

[1] Stallings, W. 1999. Cryptography and network security. Upper Saddle River, NJ: Prentice Hall Press.

[2] Baldwin, D. 2018. Simple solver software (version 5.4.5). University of California, Berkeley. Accessed February 28, 2018. https://www.simplesolverlogic.com/

[3] Mano, M., and M. Ciletti. 2013. Digital design With an Introduction to the Verilog HDL. Upper Saddle River, NJ: Pearson Press.

[4] Balch, M. 2003. Complete digital design. New York City, NY: McGraw-Hill Press.

[5] Courtois, N., and J. Pieprzyk. 2002. Cryptanalysis of block ciphers with over-defined systems of equations. Paper presented at International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT 2002, Queenstown, New Zealand, December 3.

[6] Courtois, N., A. Klimov, J. Patarin, and A. Shamir. 2000. Efficient algorithms for solving overdefined system of multivariate polynomial equations. Paper presented at International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2000, Bruges, Belgium, May 12.

[7] Abdelmageed, W. 2011. Improvements for the XL algorithm with applications to algebraic cryptanalysis. PhD diss., Darmstadt University of Technology, Faculty of Computer Science.

[8] Mitchell, C. 2016. On the security of 2-key triple DES. IEEE Transactions on Information Theory, 11, (62):1–8. doi:10.1109/TIT.2016.2611003.

[9] Abdelwahab, M., M. Rizk, El-S. El-Badawy, and H. Selim. 2018. Algebraic Cryptanalysis on MIFARE Ultralight C. Journal of Engineering Technology, 2, (6), pp. 377–393

[10] Heys, H. 2002. A tutorial on linear and differential cryptanalysis. Journal of Cryptologia, 3, (26):189–221. doi:10.1080/0161-110291890885.

[11] Kaminsky, A., M. Kurdziel, and S. Radziszowski. 2010. An overview

of cryptanalysis research for the Advanced Encryption Standard. Paper presented at IEEE Military Communication Conference MILCOM 2010, San Jose, CA, USA, November 1.

[12] Courtois, N., and G. Bard. 2007. Algebraic cryptanalysis of the Data Encryption Standard. Paper presented at 11th IMA International Conference on Cryptography and Coding, Cirencester, UK, December 20.