Defence Science Journal, Vol. 74, No. 5, September 2024, pp. 651-661, DOI : 10.14429/dsj.74.19601

MILP-Based Differential Cryptanalysis on IVLBC and Eslice-64

Manjeet Kaur* and Dhananjoy Dey

Department of Mathematics, Indian Institute of Information Technology, Lucknow - 226 002, India

**E-mail: rmm21101@iiitl.ac.in*

ABSTRACT

Lightweight block ciphers provide security to resource-limited devices. However, many of these ciphers lack security analysis against basic attacks. This paper provides a detailed security analysis of two lightweight block ciphers, IVLBC and Eslice-64, against differential attack. The designers of IVLBC and Eslice-64 claimed that their ciphers were secure against differential attack. In this paper, to substantiate existing cryptanalysis's claims, we perform differential attack on these two ciphers using the Mixed-Integer Linear Programming (MILP) method. We incorporate the Difference Distribution Table (DDT) probabilities into MILP models. We discover differential distinguishers up to seven and 15 rounds for IVLBC and Eslice-64, respectively. We improve the known distinguishers for Eslice-64 by one round. Further, we mount the key recovery attack on an eight-round IVLBC and a 16-round Eslice-64 with data/memory/time complexities of 2^{49}/ $2^{50.59}$/2^{49} and 2^{63}/$2^{12.58}$/2^{63} respectively.

Keywords: Differential cryptanalysis; Eslice-64; IVLBC; Lightweight Block Cipher; MILP

NOMENCLATURE

K	: Key
RK_i	: i^{th} round key
X	: 64-bit input block
U	: Output of add round key
V	: Output of sub cells (S-box)
Z	: Output of permute nibbles (P-box)
L	: Output of mix columns
ΔX	: Input difference
ΔY	: Output difference
Ns / $N_{r,S}$	: Number of S-boxes in the entire trail or r^{th} round
SPN	: Substitution-permutation network
N_{AS}	: Number of active S-boxes in a trail

1. INTRODUCTION

Huang[1], *et al.* designed IVLBC, a lightweight block cipher with two variants, IVLBC-80 and IVLBC-128, which depend on the key size, in 2022. Meanwhile, Li-fang[2], *et al.* introduced Eslice, a lightweight block cipher with three variants, Eslice-64-64, Eslice-64-128, and Eslice-128-128, depending on the block and key sizes, in 2023. We consider block ciphers secure if they resist attacks over the years. The security analysis of block ciphers is currently crucial against linear/differential attacks[3]. In differential attack, the attacker seeks high-probability differential trails. Nowadays, we use the MILP method in differential cryptanalysis. Many lightweight block ciphers, like ANU-II[4], Midori64[5], and PIPO-64/128[6] etc. have been analyzed against differential attack using MILP. This method represents the operations of block ciphers in terms of linear inequalities and then uses the resulting inequalities as constraints on an objective function.

Zhang and Zhang[7] analyzed the lightweight block cipher Skinny for differential attack using the MILP program. The authors provided an 11-round differential trail with the minimum active S-boxes. Then, Zhu[8], *et al.* provided the differential cryptanalysis on round-reduced GIFT using MILP. Zhou[9], *et al.* improved the MILP algorithm using the divide-and-conquer technique to assess the security of differential and linear attacks. Using this algorithm, the authors analyzed the block ciphers TWINE, RECTANGLE, PRESENT, LBLOCK, and GIFT-64. After that, Kumar and Yadav[10] analysed the differential attack on WARP using the MILP model. İlter and Selçuk[11] provided a more efficient method to write multiple XOR in terms of linear inequalities in the MILP method. Using this method, the authors provided the minimum number of active S-boxes (#AS) and high-probability differential trails of KLEIN and PRINCE. Next, İlter and Selçuk[12] analysed the cryptanalysis of FUTURE using the MILP method. The authors discovered an efficient approach for representing n-XOR using only one constraint. Then, Shiraya[13], *et al.* examined the security of Tiaoxin-346, Rocca, and AEGIS against differential attack using the MILP method. For IVLBC, İlter and Selçuk[14] identified the seven-round differential and linear characteristics with a probability of 2^{-46} and a bias of 2^{-24}, respectively. This paper contributes to the differential cryptanalysis of two lightweight block ciphers, IVLBC and Eslice-64.

1.1 Contributions

The designers of IVLBC and Eslice-64 claimed that their ciphers were resistant to differential attack, providing

Received : 10 November 2023, Revised : 07 April 2024
Accepted : 02 May 2024, Online published : 19 September 2024

nine-round and 16-round differential trails for IVLBC and Eslice-64 with probabilities of 2^{-66} and 2^{-70}, respectively. After that, İlter and Selçuk[14] determined a seven-round differential characteristic with a probability of 2^{-46} for IVLBC. On both ciphers, there has been no key recovery differential attack so far. This paper studies the MILP-based security analysis to validate these claims and find optimal differential trails for both ciphers, incorporating the Difference Distribution Table (DDT) probabilities and additional constraints on the number of active S-boxes. This paper also presents the key recovery differential attack on IVLBC and Eslice-64. Our contributions are as follows:

- For IVLBC, we provide the minimum active S-boxes and probabilities of optimal differential trails up to nine rounds. There are differential distinguishers for IVLBC up to seven rounds. Specifically, we present a seven-round differential trail for IVLBC with 23 minimum active S-boxes and a probability of 2^{-46}
- For Eslice-64, we provide the minimum active S-boxes and probabilities of optimal differential trails up to 16 rounds. Eslice-64's designers found differential distinguishers up to 14 rounds. However, we discover differential distinguishers up to 15 rounds in our paper. In addition, we give a 15-round differential trail for Eslice-64 with 30 minimum active S-boxes and a probability of 2^{-60}.
- Moreover, we introduce a key recovery attack on an eight-round IVLBC and a 16-round Eslice-64 with data/memory/time complexities of $2^{49}/2^{50.59}/2^{49}$ and $2^{63}/2^{12.58}/2^{63}$ respectively.

1.2 Organization

The following is the outline of the remaining paper: Section 2 discusses the IVLBC and Eslice-64 lightweight ciphers. We create MILP models for differential attack in Section 3. Section 4 provides differential trails and key recovery attacks on IVLBC and Eslice-64. Finally, Section 5 provides the conclusion of the paper.

2. IVLBC AND ESLICE-64

This section discusses the two lightweight block ciphers, IVLBC and Eslice-64, depending on SPN and Feistel structures, respectively.

2.1 IVLBC

IVLBC operates on a 64-bit block with an 80/128-bit key. This section describes the round function and the key generation procedure of IVLBC.

Table 1. S-box (IVLBC)

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(t)$	0	15	14	5	13	3	6	12	11	9	10	8	7	4	2	1

Table 2. P-box (IVLBC)

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(t)$	0	7	10	13	4	11	14	1	8	15	2	5	12	3	6	9

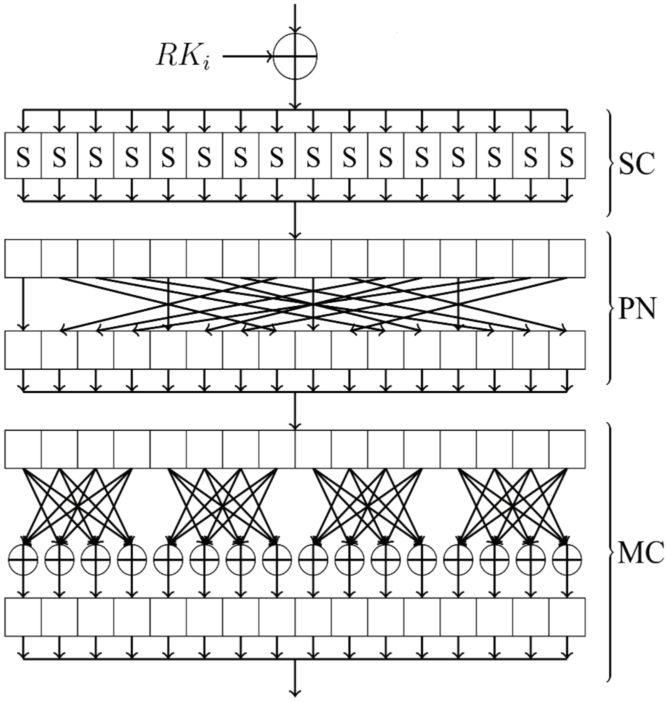


Figure 1. IVLBC round function.

2.1.1 *Round Function*

IVLBC has 29 rounds. Each round function of IVLBC comprises AddRoundKey (ARK), SubCells (SC), PermuteNibbles (PN), and MixColumns (MC), consecutively, as shown in Fig. 1. In the last round, there is only an AddRoundKey operation. Here, we describe the operations of the round function.

2.1.1.1 Add Round Key

This operation performs XOR between a 64-bit block (X) and the 64-bit high of RK_i, such as:

$$U = X \oplus RK_i \tag{1}$$

2.1.1.2 Sub Cells

First, divide a 64-bit block (U) into 16 subblocks $(U_j, 0 \le j \le 15)$, and each subblock has a length of 4 bits. Then, use the same S-box (Table 1) on each subblock as follows:

$$V_j = S(U_j), 0 \le j \le 15 \tag{2}$$

2.1.1.3 Permute Nibbles

In this operation, write a 64-bit block (V) into 16 subblocks $(V_j, 0 \le j \le 15)$ of length 4 bits. Then, applying the permutation as given in Table 2, we get:

Table 3. S-box (Eslice)

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(t)$	6	0	8	15	12	3	7	13	11	14	1	4	5	9	10	2

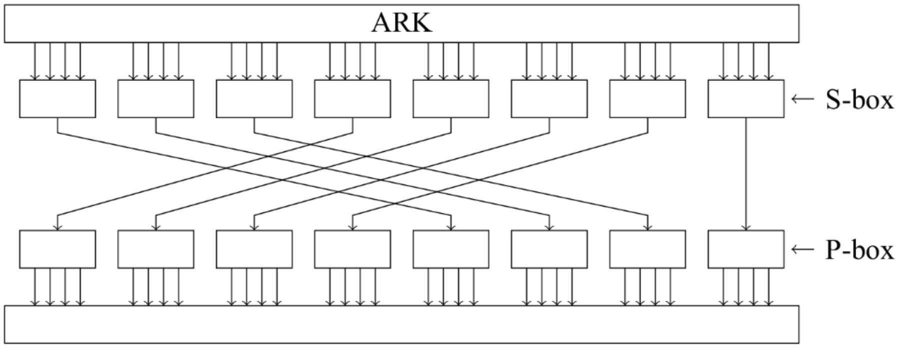


Figure 2. Eslice-64 round function.

$$Z_j = P(V_j), 0 \le j \le 15 \tag{3}$$

2.1.1.4 Mix Columns

First, represent a 64-bit input block (Z) of MixColumns into a 4×4 matrix. Then, $L=M\times Z$ is the output of MixColumns, where:

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

2.1.2 Key Generation

Consider the key is $K= K_0K_1K_2K_3$ where, the length of $K_i (0 \le i \le 3)$ is 20/32-bit for an 80/128-bit key, respectively. For IVLBC-80, first, apply an 11-bit left circular shift to K_0K_1, Then, substitute four bits (k_{76}-k_{79}) using an S-box (as shown in Table 1). Subsequently, perform XOR between five bits (k_{40}-k_{44}) and RC_i, where, $RC_i \in \{1,2,3,...,29\}$. Finally, update the key K by $K_2K_3K_0K_1$ (Algorithm 1). Similarly, there is a key generation procedure for IVLBC-128, as shown in Algorithm 2.

Algorithm 1: Key Generation Algorithm of IVLBC-80

```
Data: $K$
  Result: $RK$
  for $i = 1$ to $29$ do
    $K_0K_1K_2K_3 \leftarrow K;$
    $K_0K_1 \leftarrow (K_0K_1) <<< 11;$
    $[k_{76} : k_{79}] \leftarrow S([k_{76} : k_{79}]);$
    $[k_{40} : k_{44}] \leftarrow [k_{40} : k_{44}] \oplus RC_i;$
    $RK_i \leftarrow K_2K_3K_0K_1;$
    $K \leftarrow RK_i;$
  end
  return $RK$
```

Algorithm 2: Key Generation Algorithm of IVLBC-128

```
Data: $K$
  Result: $RK$
  for $i = 1$ to $29$ do
    $K_0K_1K_2K_3 \leftarrow K;$
    $K_0K_1 \leftarrow (K_0K_1) <<< 7;$
    $[k_{120} : k_{123}] \leftarrow S([k_{120} : k_{123}]);$
    $[k_{124} : k_{127}] \leftarrow S([k_{124} : k_{127}]);$
    $[k_{64} : k_{68}] \leftarrow [k_{64} : k_{68}] \oplus RC_i;$
    $RK_i \leftarrow K_2K_3K_0K_1;$
    $K \leftarrow RK_i;$
  end
  return $RK$
```

2.2 Eslice-64

Eslice-64 has 35 (or 38) rounds of Eslice-64-64 (or Eslice-64-128), respectively. Eslice-64 operates on a 64-bit block with a 64/128-bit key. Here, we describe the round function and the key generation procedure as follows:

2.2.1 Round Function

This function consists of AddRoundKey, S-box, and P-box, as shown in Fig. 2. We discuss the operations of the round function as follows:

2.2.2 Add Round Key

First, divide a 64-bit block (X) into two subblocks of length 32 bits ($X=X_{j-1}X_j$). Then, perform XOR between a 32-bit left subblock (X_{j-1}) and a 32-bit round key (RK_i) as follows:

$$U = X_{j-1} \oplus RK_i \tag{4}$$

2.2.3 S-box

First, write a 32-bit block (U) into eight nibbles ($U_j, 0 \le j \le 7$). Then, use an S-box (Table 3) on each nibble, as given below:

$$V_j = S(U_j), 0 \le j \le 7 \tag{5}$$

2.2.4 P-box

First, divide a 32-bit block into eight nibbles, that is, $V=V_0V_1\ldots V_7$. We then apply the P-box as shown in Table 4. Finally, we have:

$$Z_j = P(V_j), 0 \le j \le 7 \tag{6}$$

Table 4. P-box (Eslice)

t	0	1	2	3	4	5	6	7
$P(t)$	3	4	5	6	0	1	2	7

2.2.2 Key Generation

Consider $K=k_0k_1k_2\dots k_{63}$ for Eslice-64-64. First, perform a 49-bit left circular shift on K. Then, apply the S-box (see Table 3) to the leftmost four bits (k_0–k_3). Subsequently, perform XOR between five bits (k_{28}–k_{32}) and the round constant R_i. Here, we obtain the round constant R_i using a five-bit LFSR[2], where the initial state R_1 is $0x1$. Finally, the first 32 bits of the updated key K form a round key, as shown in Algorithm 3. Similarly, we have the key generation algorithm of Eslice-64-128[2].

Algorithm 3: Key Generation Algorithm of Eslice-64-64

```
Data: $K$
Result: $RK$
for $i = 1$ to $35$ do
    $K \leftarrow K <<< 49;$
    $[k_0 : k_3] \leftarrow S([k_0 : k_3]);$
    $[k_{28} : k_{32}] \leftarrow [k_{28} : k_{32}] \oplus R_i;$
    $RK_i \leftarrow K_0K_1K_2 ... k_{31};$
end
return $RK$
```

3. MILP MODEL

This section discusses the linear inequalities corresponding to operations, such as XOR, Permutation, MixColumns, and S-boxes to create MILP models (.lp format).

3.1 XOR

Suppose $z = x \oplus y$, where, (x,y) and z are the input and output bit differences of XOR, respectively. The linear inequalities of XOR are given by

$$\begin{cases} x+y+z \geq 2d \\ x \leq d \\ y \leq d \\ z \leq d \\ x+y+z \leq 2 \end{cases} \tag{7}$$

where, $d \in \{0,1\}$.

3.2 Permutation

Consider the input and output differences of P are $(x_1,x_2,x_3,\dots,x_{64})$ and $(y_1,y_2,y_3,\dots,y_{64})$, respectively. Therefore, $y_j = P(x_j), 1 \leq j \leq 64$ are linear equations of the permutation operation.

3.3 MixColumns

The matrix (M) of MixColumns for IVLBC is given by:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

First, we convert the matrix M into a bit matrix of order 16 as follows:

$$\begin{pmatrix}
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1\\
1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1\\
1&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1\\
1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0
\end{pmatrix}$$

Consider $(y_1,y_2,y_3,\dots,y_{64})$ and $(z_1,z_2,z_3,\dots,z_{64})$ as input and output differences of MixColumns operation, respectively. There are 32 intermediate variables and 384 linear inequalities that describe the MixColumns operation. For example, $z_1 = y_5 \oplus y_9 \oplus y_{13}$. Define $d_1 = y_5 \oplus y_9$, then $z_1 = d_1 \oplus y_{13}$. Therefore, the linear inequalities for z_1 are defined as follows:

$$\begin{cases} d_1 + y_5 + y_9 \leq 2 \\ d_1 + y_5 - y_9 \geq 0 \\ d_1 - y_5 + y_9 \geq 0 \\ -d_1 + y_5 + y_9 \geq 0 \\ z_1 + d_1 + y_{13} \leq 2 \\ z_1 + d_1 - y_{13} \geq 0 \\ z_1 - d_1 + y_{13} \geq 0 \\ -z_1 + d_1 + y_{13} \geq 0 \end{cases} \tag{8}$$

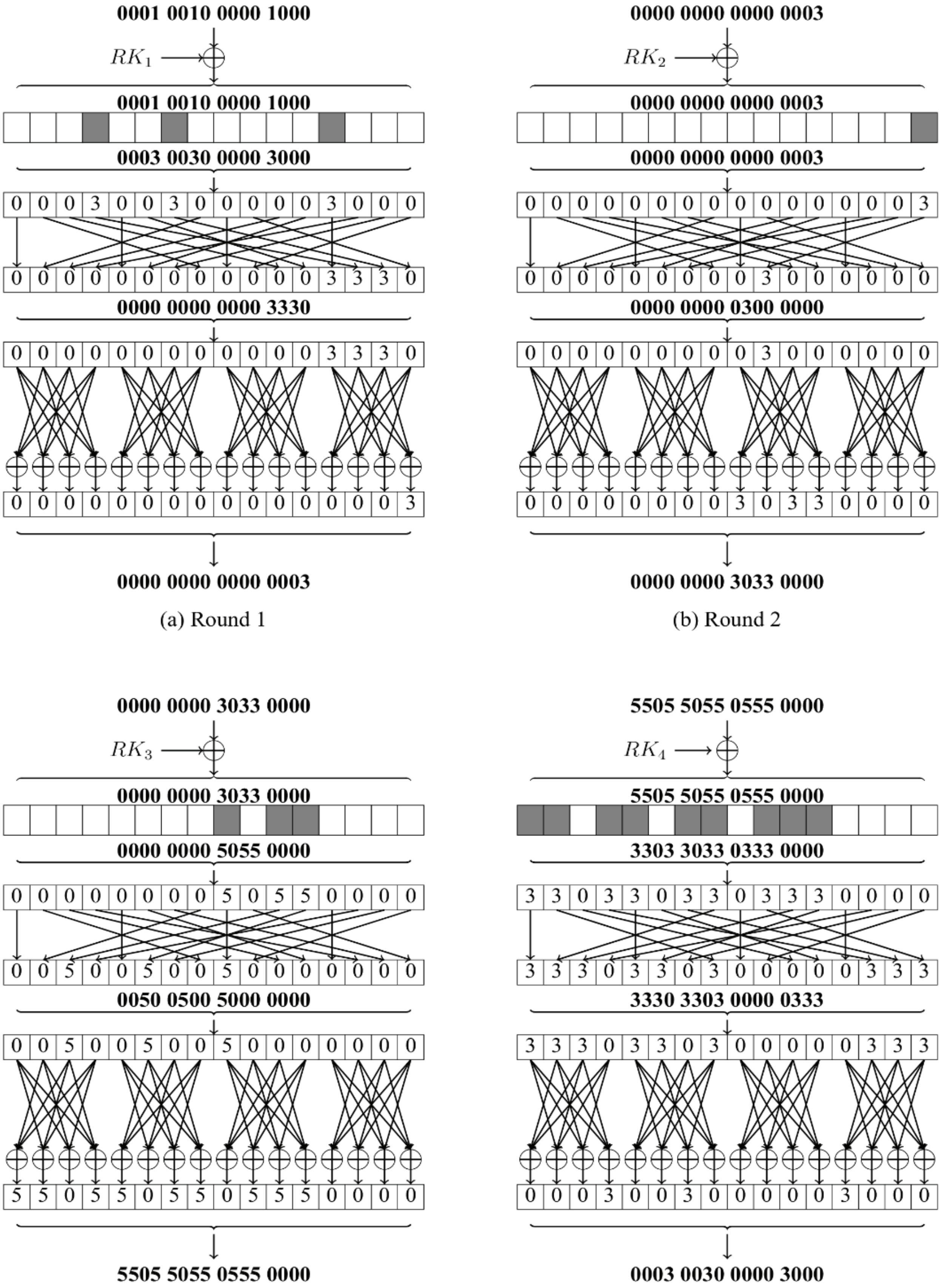
3.4 S-box

3.4.1 S-box Linear Inequalities

Consider the input and output differences are (x_1,x_2,x_3,x_4) and (y_1,y_2,y_3,y_4), respectively of a 4×4 S-box. Consider a binary

Table 5. Differentially active S-boxes and probabilities of optimal trails (IVLBC)

Round	N_{AS}	Probability	#Variables		#Constraints	
			This paper	İlter and Selçuk[14]	This paper	İlter and Selçuk[14]
1	1	2^{-2}	320	432	579	561
2	4	2^{-8}	560	800	1076	1121
3	7	2^{-14}	800	1168	1573	1681
4	16	2^{-32}	1040	1536	2070	2241
5	17	2^{-34}	1280	1904	2567	2801
6	20	2^{-40}	1520	2272	3064	3361
7	23	2^{-46}	1760	2640	3561	3921
8	32	2^{-64}	2000	-	4058	-
9	33	2^{-66}	2240	-	4635	-

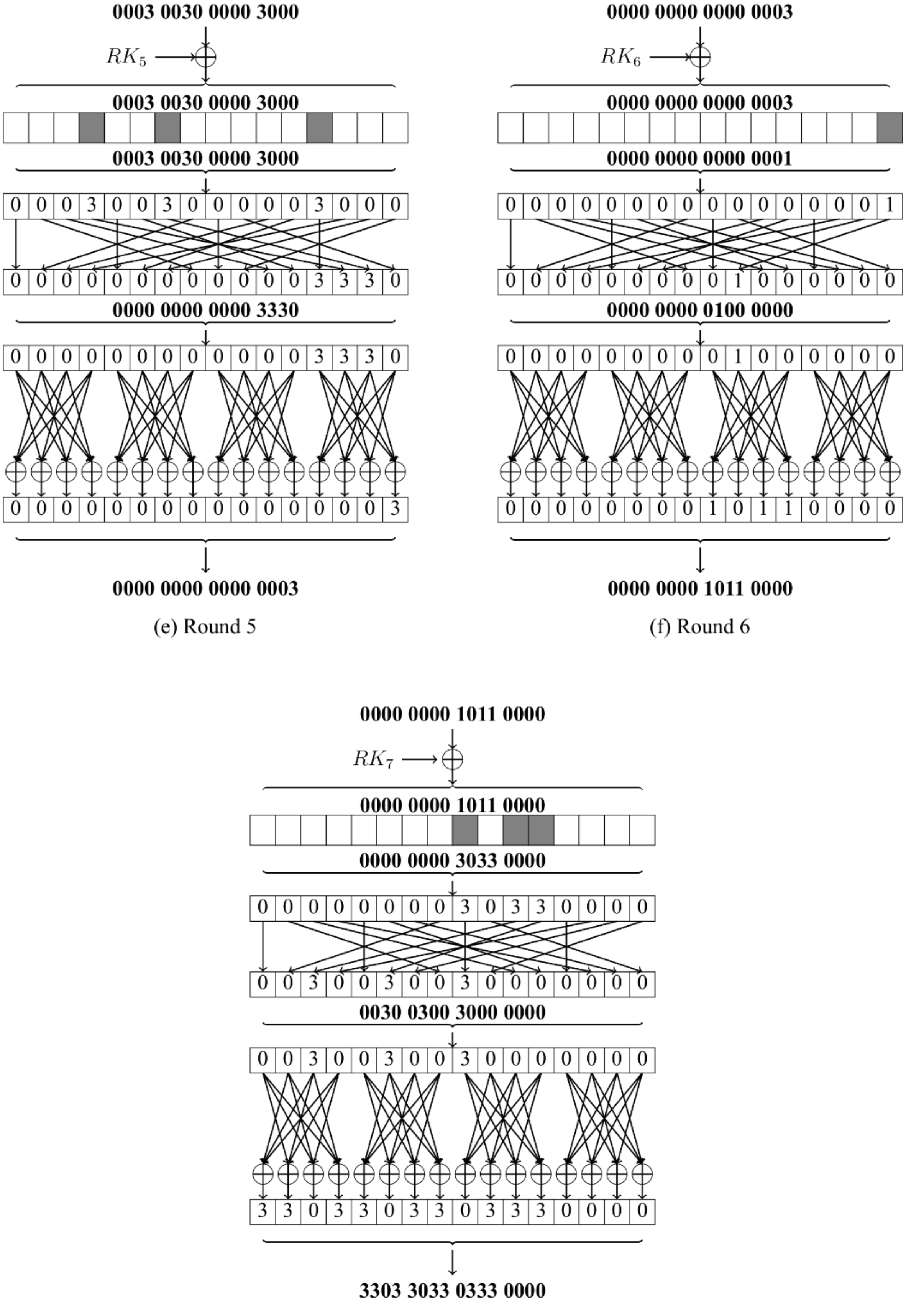


(a) Round 1

(b) Round 2

(c) Round 3

(d) Round 4



(e) Round 5

(f) Round 6

(g) Round 7

Figure 3. The Seven-round Differential Trail of IVLBC.

variable A_i to represent the i^{th} S-box, that is, A_i=1 if and only if all x_j are not zero. We then incorporate the following linear inequalities into MILP models:

$$\begin{cases} \sum_{j=1}^{4} x_j - A_i \geq 0 \\ A_i - x_j \geq 0, 1 \leq j \leq 4 \end{cases} \quad (9)$$

Consider an input-output differential of the S-box as a point $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) \in \mathbb{F}_2^8$. There are 97 and 159 possible and impossible points in the DDT of IVLBC and Eslice-64, respectively. Then, generate the linear inequalities corresponding to all possible input-output differential points of the S-box using the double description method[1]. There are 198 and 237 linear inequalities of S-boxes for IVLBC and Eslice-64, respectively. Then, there are only 21 and 22 linear inequalities of S-boxes for IVLBC and Eslice-64 (see on GitHub) using MILP method[15] and Gurobi solver, respectively.

3.4.2 S-box Linear Inequalities Including Probabilities

There are only three nonzero values: 16, 4, and 2 in DDT of S-boxes for IVLBC and Eslice-64. Therefore, we require two binary variables (p_1,p_2) to define new differentials with probabilities $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, p_1, p_2) \in \mathbb{F}_2^{10}$ as shown in Eqn (10). The double description method provides 363 and 477 linear inequalities of S-boxes for IVLBC and Eslice-64, respectively. Similar to Section 3.4.1, there are 20 linear inequalities for S-boxes of both ciphers (see on GitHub).

$$(p_1, p_2) = \begin{cases} (0,1)\ if\ DDT[\Delta_i, \Delta_o] = 2 \\ (1,0)\ if\ DDT[\Delta_i, \Delta_o] = 4 \\ (0,0)\ if\ DDT[\Delta_i, \Delta_o] = 16 \end{cases} \quad (10)$$

3.5 Objective Function

The objective functions are defined as $\min \sum_{i=1}^{N_S} A_i$ and $\min \sum_{i=1}^{N_{AS}} (2p_1 + 3p_2)$.

3.6 Additional Constraints

There are more variables and constraints in the model when we introduce further rounds. Consequently, the solution time increases exponentially. For the analysis of FUTURE, İlter and Selçuk[12] employed additional restrictions on their model that bound differentially active S-boxes in each round. To achieve differential trails for IVLBC and Eslice-64, we impose additional restrictions such as $\sum_{i=1}^{N_S} A_i \geq \min$ and $\sum_{i=1}^{N_{r,S}} A_i \leq \max$ to bound the #AS in the entire trail and each round, respectively.

4. DIFFERENTIAL CRYPTANALYSIS

This section provides differential trails for IVLBC and Eslice-64 using MILP models. The Python codes are available on GitHub[2]. Moreover, we mount the key recovery attack on both ciphers[16].

4.1 IVLBC

The minimum differentially active S-boxes and probabilities of optimal trails up to nine rounds are provided in Table 5. From Table 5, we conclude that there are differential distinguishers up to seven rounds—since $2^{-p} > 2^{-64}$. Moreover, Table 5 shows that our MILP models have less number of variables and constraints (except round one) as compared to İlter and Selçuk's models. Further, there is a detailed seven-round trail with 23 minimum active S-boxes and a probability of 2^{-46} in Table 6 and Fig. 3. There is a nine-round trail with a probability of 2^{-66}($<2^{-64}$). As a result, full-round IVLBC is resistant to differential attack.

Table 6. Seven-round differential trail of IVLBC (input difference = 0001 0010 0000 1000)

Round	Output difference	Probability
1	0000 0000 0000 0003	2^{-6}
2	0000 0000 3033 0000	2^{-8}
3	5505 5055 0555 0000	2^{-14}
4	0003 0030 0000 3000	2^{-32}
5	0000 0000 0000 0003	2^{-38}
6	0000 0000 1011 0000	2^{-40}
7	3303 3033 0333 0000	2^{-46}

Table 7. Key recovery attack on an eight-round IVLBC (input difference = 0001 0010 0000 1000)

Round	Output difference
1	0000 0000 0000 0003
2	0000 0000 3033 0000
3	5505 5055 0555 0000
4	0003 0030 0000 3000
5	0000 0000 0000 0003
6	0000 0000 1011 0000
7	3303 3033 0333 0000
8	???? ???? 0000 ????

Table 8. Differentially active S-boxes and probabilities of optimal trails (Eslice-64)

Round		1	2	3	4	5	6	7	8
This Paper	N_{AS}	0	1	2	3	4	6	7	9
	Probability	2^{-0}	2^{-2}	2^{-4}	2^{-6}	2^{-8}	2^{-12}	2^{-14}	2^{-18}
Li-fang *et al.*[2]	N_{AS}	0	1	2	3	4	6	8	10
	Probability	2^{-0}	2^{-2}	2^{-4}	2^{-6}	2^{-8}	2^{-12}	2^{-16}	2^{-18}
Round		9	10	11	12	13	14	15	16
This Paper	N_{AS}	12	15	18	22	25	27	30	33
	Probability	2^{-24}	2^{-30}	2^{-36}	2^{-44}	2^{-50}	2^{-54}	2^{-60}	2^{-66}
Li-fang *et al.*[2]	N_{AS}	12	14	17	20	23	27	31	34
	Probability	2^{-24}	2^{-30}	2^{-38}	2^{-45}	2^{-53}	2^{-59}	2^{-64}	2^{-70}

4.1.1 Key Recovery Attack on Eight-Round IVLBC

We exploit the seven-round trail (see Table 6) for a key recovery attack on an eight-round IVLBC, where ΔX=0001 001000001000 and ΔY=3303 3033 0333 0000. We add another round to this trail and consider the output difference as ΔC. There are 48 unknown and 16 fixed bits in ΔC (Table 7). The following is the attack procedure:

- Encrypt 2^{48} pairs of plaintexts to obtain at least $2^{48-46}=2^2$ right pairs that satisfy the trail.
- In ΔC, there are 16 fixed bits to filter out incorrect pairs. After filtering, there are $2^{48-16}=2^{32}$ pairs.
- Set 2^{48} counters and estimate 48 bits of round key corresponding to unknown bits in ΔC.
- Increase the key counter corresponding to the particular round key if a one-round partial decryption with that key yields ΔY. For increment in the correct round key counter, there are at least four correct pairs.

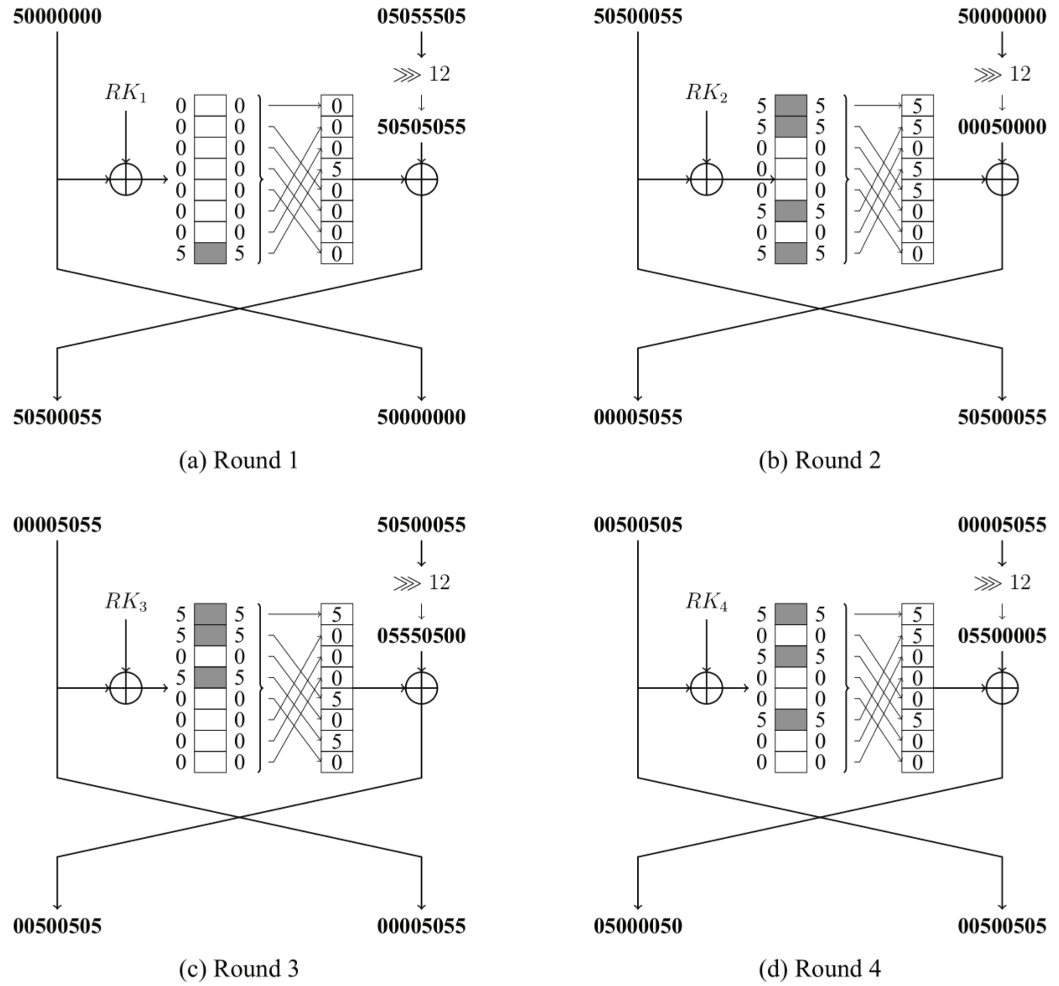
We are required to encrypt 2^{49} chosen plaintexts (D=2^{49}), therefore, T=2^{49} is the time complexity. We need the memory, which is $M = 48\times\frac{2^{48}}{8} = 2^{50.59}$ bytes to store 2^{48} 48-bit round keys. The probability of successfully retrieving the right one-round key with four correct pairs is $1-e^{-2^{48-46}} = 0.982$.

Table 9. 15-round differential trail of eslice-64 (input difference = 50000000 05055505)

Round	Output difference	Probability
1	50500055 50000000	2^{-2}
2	00005055 50500055	2^{-10}
3	00500505 00005055	2^{-16}
4	05000050 00500505	2^{-22}
5	50550000 05000050	2^{-26}
6	55000050 50550000	2^{-32}
7	00005050 55000050	2^{-38}
8	00005000 00005050	2^{-42}
9	00000005 00005000	2^{-44}
10	00000000 00000005	2^{-46}
11	00500000 00000000	2^{-46}
12	00000050 00500000	2^{-48}
13	00050500 00000050	2^{-50}
14	55500000 00050500	2^{-54}
15	50005500 55500000	2^{-60}

4.2 Eslice-64

The minimum differentially active S-boxes and probabilities of optimal trails up to 16 rounds are shown in Table 8. From Table 8, there are differential distinguishers up to 15 rounds, whereas designers distinguishers are up to 14 rounds. In addition, there is a detailed 15-round trail with 30 minimum active S-boxes and a probability of 2^{-60} in Table 9

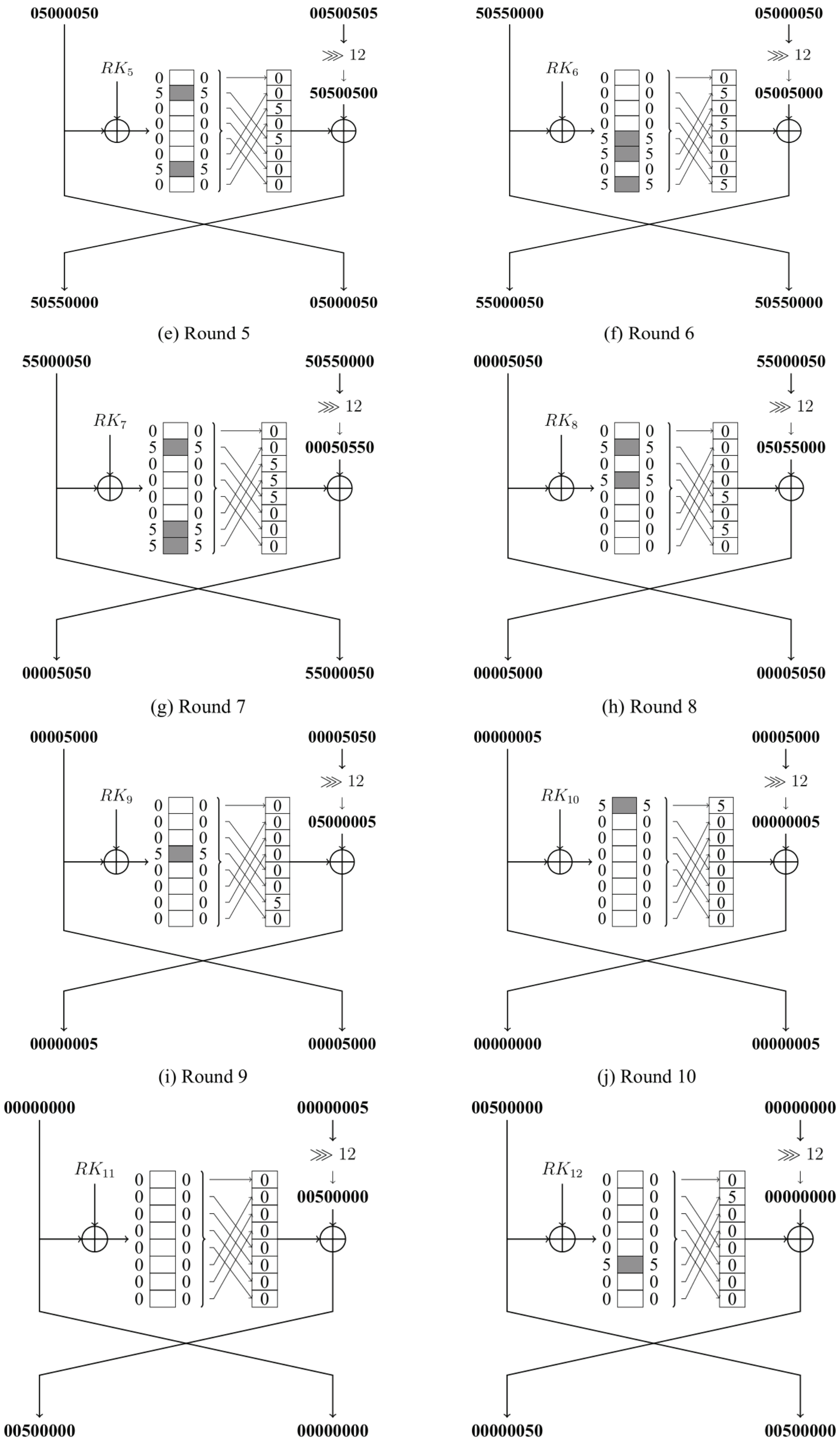


(a) Round 1

(b) Round 2

(c) Round 3

(d) Round 4



(e) Round 5

(f) Round 6

(g) Round 7

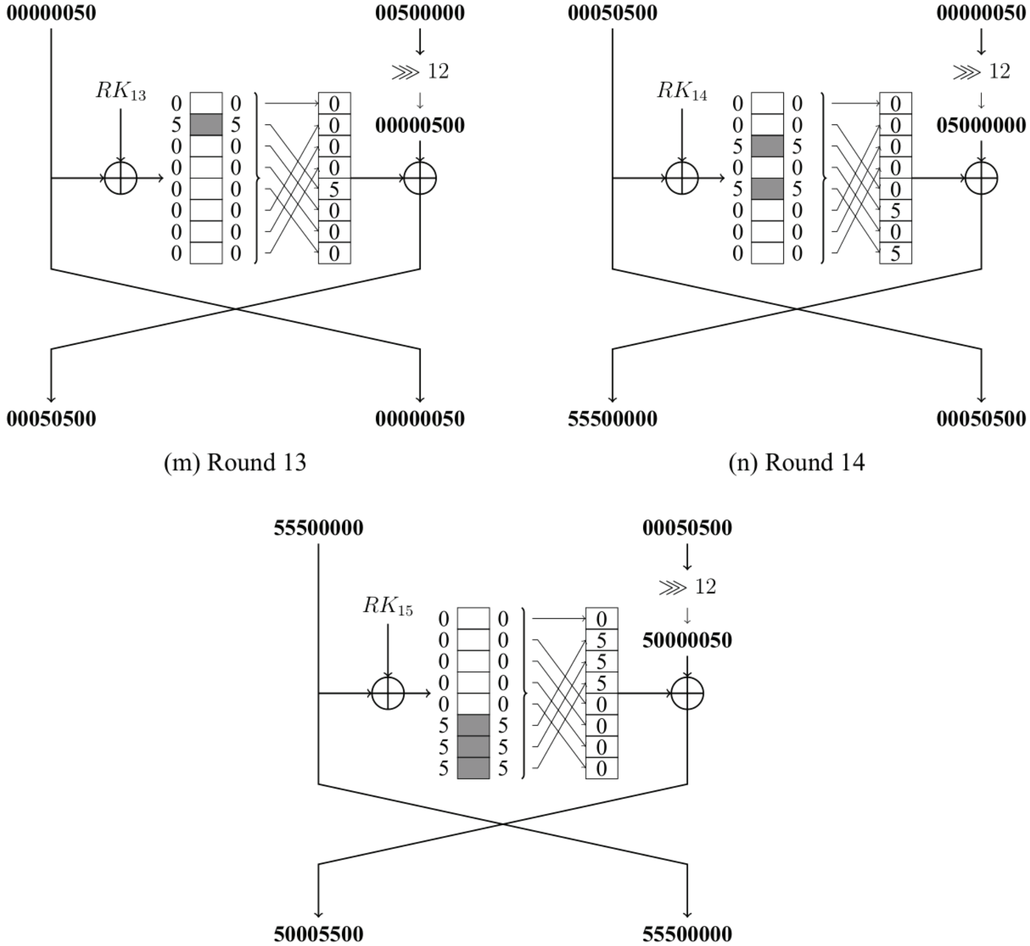
(h) Round 8

(i) Round 9

(j) Round 10

(k) Round 11

(l) Round 12



(m) Round 13

(n) Round 14

(o) Round 15

Figure 4. 15 rounds differential trail of Eslice-64.

and Fig. 4. The probability of a 16-round trail is $2^{-66}(<2^{-64})$. Consequently, full-round Eslice-64 is sufficiently secure against differential attack.

4.2.1 *Key Recovery Attack on 16-round Eslice-64*

We take an optimal 15-round trail (see Table 9) for the key recovery attack on a 16-round Eslice-64, where ΔX=5000000005055505 and ΔY=5000550055500000. We append a further round to this trail and assume that the output difference is ΔC. Similar to Section 4.1.1., we encrypt 2^{62} pairs of plaintexts to obtain at least $2^{62-60}=2^2$ correct pairs. There are 12 active and 52 fixed bits in ΔC (see Table 10). After filtration with 52 fixed bits, there are only $2^{62-52}=2^{10}$ pairs. We consider 2^{12} counters to guess the 12 bits of the round key. Therefore, the time, data, and memory complexities are $T=2^{63}$, $D=2^{63}$, and $M=2^{12.58}$ bytes, respectively. The attack has a probability $1-e^{-2^{62-60}}=0.982$ of obtaining a one-round key with four right pairs.

5. CONCLUSION

In our paper, we have created MILP models to find the single-key differential trails for two lightweight block ciphers, IVLBC and Eslice-64. We have included DDT probabilities to create MILP models. Through MILP models, we have discovered differential distinguishers up to seven rounds for

Table 10. Key recovery attack on a 16-round Eslice-64 (Input difference = 50000000 05055505)

Round	Output difference
1	50500055 50000000
2	00005055 50500055
3	00500505 00005055
4	05000050 00500505
5	50550000 05000050
6	55000050 50550000
7	00005050 55000050
8	00005000 00005050
9	00000005 00005000
10	00000000 00000005
11	00500000 00000000
12	00000050 00500000
13	00050500 00000050
14	55500000 00050500
15	50005500 55500000
16	0??5?500 50005500

IVLBC. Similarly, we have identified differential distinguishers for Eslice-64 up to 15 rounds. For Eslice-64, our distinguishers cover one more round than previously known distinguishers. Moreover, we have mounted the key recovery attack on an eight-round IVLBC and a 16-round Eslice-64 with data/memory/time complexities of 2^{49}/$2^{50.59}$/2^{49} and 2^{63}/$2^{12.58}$/2^{63} respectively.

REFERENCES

1. Huang, X.; Li, L. & Yang, J. IVLBC: An involutive lightweight block cipher for internet of things. *IEEE Syst. J.*, 2022.
   doi: 10.1109/JSYST.2022.3227951
2. Li-fang, L.; Xiao-ni, D.U.; Kai-bin, L.I.; Xin, X.I.E. & Xiao-dan, L.I. Block cipher algorithm Eslice based on Feistel structure. *J. SHANDONG Univ. Sci.*, 2023.
   doi: 10.6040/j.issn.1671-9352.0.2022.283
3. Heys, H.M. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 2002, **26**(3).
   doi: 10.1080/0161-110291890885
4. Fan, T.; Li, L.; Wei, Y. & Pasalic, E. Differential cryptanalysis of full-round ANU-II ultra-lightweight block cipher. *Int. J. Distrib. Sens. Networks*, 2022, **18**(9).
   doi: 10.1177/15501329221119398
5. Zhao, H.; Han, G.; Wang, L. & Wang, W. MILP-based differential cryptanalysis on round-reduced midori64. *IEEE Access*, 2020, **8**.
   doi: 10.1109/ACCESS.2020.2995795
6. Yadav, T. & Kumar, M. Modeling large S-box in MILP and a (Related-Key) differential attack on full round PIPO-64/128. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics) 2022.
   https://eprint.iacr.org/2021/1388
7. Zhang, P. & Zhang, W. Differential cryptanalysis on block cipher skinny with MILP program. *Secur. Commun. Networks*, 2018.
   doi: 10.1155/2018/3780407
8. Zhu, B.; Dong, X. & Yu, H. MILP-based differential attack on round-reduced GIFT. In: Topics in Cryptology–CT-RSA 2019: The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4–8, 2019, Proceedings 2019. p. 372–90.
   doi: 10.1007/978-3-030-12612-4_19
9. Zhou, C.; Zhang, W.; Ding, T. & Xiang, Z. Improving the MILP-based security evaluation algorithm against differential/linear cryptanalysis using a divide-and-conquer approach. *Cryptol. EPrint Arch.*, 2019.
   https://eprint.iacr.org/2019/019
10. Kumar, M. & Yadav, T. MILP based differential attack on round reduced WARP. *In* International Conference on Security, Privacy, and Applied Cryptography Engineering 2021, PP. 42–59.
    doi: 10.1007/978-3-030-95085-9_3
11. İlter, M.B. & Selçuk, A.A. A new MILP model for matrix multiplications with applications to KLEIN and PRINCE. In: SECRYPT 2021, 420–7.
    doi: 10.5220/0010519504200427
12. İlter, M.B. & Selçuk, A.A. MILP-aided Cryptanalysis of the FUTURE block cipher. *In* International Conference on Information Technology and Communications Security 2022, PP. 153–67.
    doi: 10.1007/978-3-031-32636-3_9
13. Shiraya, T.; Takeuchi, N.; Sakamoto, K. & Isobe, T. MILP-based security evaluation for AEGIS/Tiaoxin-346/Rocca. *IET Inf. Secur.*, 2023, **17**(3), 458–67.
    doi: 10.1049/ise2.12109
14. Ilter, M.B. & Aydin Selcuk, A. Differential and linear cryptanalysis of IVLBC via MILP modeling. *In* 16th International Conference on Information Security and Cryptology, ISCTURKEY 2023 - Proceedings Institute of Electrical and Electronics Engineers Inc., 2023.
    doi: 10.1109/ISCTrkiye61151.2023.10336125
15. Sasaki, Y. & Todo, Y. New algorithm for modeling S-box in MILP based differential and division trail search. *In* Innovative Security Solutions for Information Technology and Communications: 10th International Conference, SecITC 2017, Bucharest, Romania, June 8–9, 2017, Revised Selected Papers 10 2017, PP. 150–65.
    doi: 10.1007/978-3-319-69284-5_11
16. Chan, Y.Y.; Khor, C.Y.; Khoo, B.T.; Teh, J. Sen; Teng, W.J. & Jamil, N. On the resistance of new lightweight block ciphers against differential cryptanalysis. *Heliyon*, 2023, **9**(4).
    doi: 10.1016/j.heliyon.2023.e15257

CONTRIBUTORS

Ms Manjeet Kaur obtained MSc degree from Kurukshetra University, Kurukshetra, Haryana, India. She is pursuing PhD from Indian Institute of Information Technology, Lucknow, India. Her research interest includes the differential cryptanalysis of lightweight block ciphers.
In this paper, her contributions are: Formulation of MILP models, results findings, key recovery attack, and manuscript writing.

Dr Dhananjoy Dey obtained PhD from Jadavpur University, Kolkata, India. He worked as a Scientist at DRDO. Currently, he is working as an Associate Professor in IIIT Lucknow, India. His research areas include: Design and analysis of block ciphers, design and analysis of cryptographic hash functions, multivariate public key cryptography, and post quantum cryptography.
In this paper, his contribution includes supervision.