Improving Clefia and six partitions Feistel structures by Multiple MDS Matrices

Mahdi Sajadieh, Mohammad Vaziri and Ali Zaghian

***Abstract*— Counting the minimum number of differential active S-boxes is a common way to evaluate the security of block ciphers against differential and linear cryptanalysis. In this paper, we use mixed-integer linear programming (MILP) to calculate minimum number of active S-boxes of the some Feistel structures. We focus on Type-II of Feistel structures with four and six partitions and explain how to analyze them by MILP when they have more than one MDS matrices (like Clefia) in their structure. Moreover, we propose a new four partitions Feistel structure with three multiple MDS matrices which have more active S-boxes rather than Clefia structure. We also generalize Clefia structure in to six partitions Feistel structure by three multiple MDS matrices for 192 bits block size.**

***Keywords*— Clefia Structure, Linear Programming, Switching Method, Generalized Feistel Structure, Active S-boxes,**

I. INTRODUCTION

GENERALIZED Feistel structures (GFS) are one of the applicable structures for design of block ciphers which have suitable implementation properties. For instance the GFS have smaller F-functions compared to the common SPN structure (for the same block size) and also GFS do not need inverse F-function for decryption [1]. There are different types of generalizes Feistel structures according to input and output of the F-function and in this paper we focus on Type-II with SP function.

To evaluate the immunity of a cryptosystem against differential attack, counting the number of active S-boxes is a suitable method. Hitherto many algorithms have been proposed to count the minimum number of active S-boxes of Feistel structures such as [1, 2, 3].

To drive an upper bound for the probability of the best characteristic, after finding the minimum number of active S-boxes, maximum differential probability of the S-boxes are powered to the number of active S-boxes. An actual characteristic with the given number of active S-boxes may not exist. This is not a concern, since our goal is to calculate a security bound against differential cryptanalysis.

The ratio of the minimum number of active S-boxes for Feistel structures is lower than SPN structure in the specified number of rounds. It is usual, because the total number of S-boxes of Feistel structures is half of number of S-boxes in corresponding SPN structure. But the ratio of the minimum number of active S-boxes for Feistel cipher is lower than half of SPN structure in the specified number rounds. This is because of difference cancellation which always occurs in the XOR operation. To avoid these cancellations a method called *switching* has been proposed [2, 4, 5, 6, 7].

Clefia [5] is a light weight block cipher which is designed by Sony Corporation. The plaintext in the block cipher Clefia divides to four partitions. This block cipher is based on switching method where two different MDS matrices are used.

The method which we use to count the minimum number of active S-boxes for Feistel structures is based on mixed-integer linear programming. This method is derived from Mouha et al.'s method [8] that has been proposed to find lower bounds on minimum number of active S-boxes of the stream cipher Enocoro-128v2 [9]. This method only involves writing out simple linear equality and inequality constraints that are input into a MILP solver and use CPLEX software [10].

In this paper we explain how we can convert the switching mechanism in to inequalities that are used in MILP model. Moreover we propose a four partitions Feistel structure with three multiple MDS matrices which is more resistant against differential attack rather than Clefia and also generalize Clefia structure in to six partitions Feistel structure with three multiple MDS matrices.

This paper is organized as follows. In Section II some definitions are reviewed that we need. MILP method is explained for differential analysis of common Feistel structure in Section III. In Section IV we use the described method in Section III to analyze the four partitions Feistel structure with one MDS matrix and two MDS matrices (Clefia). Finally in Section V we propose the four partitions Feistel structure with three multiple MDS matrices and then we generalize Clefia structure in to six partitions Feistel structure with three multiple MDS matrices.

II. PRELIMINARIES

A. Description of standard four and six partitions Feistel structure

In this paper, we focus on the standard four and six partitions Feistel structures Type-II. In the following we describe the structure of standard four partitions structure.

Manuscript received September 15, 2016; revised September 5, 2017, accepted September 10, 2017

Mahdi Sadjadieh is with the Department of Electrical Engineering, Islamic Azad University, Isfahan (Khorasgan) Branch, Isfahan, Iran. Email: m.sajadieh@khuisf,ac,ir

Mohammad Vaziri is a graduated MSc student in the Department of Applied Science, Malek Ashtar University of Technology, Shahinshahr, Iran. Email: mohammad.vaziri67@gmail.com

Ali Zaghian is with the Department of Applied Scsience, Malek Ashtar University of Technology, Shahinshahr, Iran. Email : a_zaghian@mut-es.ac.ir

Suppose that a 4mn-bit plaintext P is divided in to 4 sub blocks as $p=(x_0^{(1)},x_1^{(1)},x_2^{(1)},x_3^{(1)})$ where $x_j^{(i)}\in\{0,1\}^{mn}$. Moreover, the output of round i+1 is calculated as follows [1]:

$$(x_0^{(i+1)},x_1^{(i+1)},x_2^{(i+1)},x_3^{(i+1)}) \leftarrow \pi(x_0^{(i)},F_1^{(i)}(x_1^{(i)})\oplus x_0^{(i)},x_1^{(i)},F_2^{(i)}(x_2^{(i)})\oplus x_3^{(i)}) \quad (1)$$

where $F_j^{(i)}:\{0,1\}^{mn}\rightarrow\{0,1\}^{mn}$ is a *j*-th round function in the *i*-th round, and π is a deterministic permutation (for example $\pi(x_0,x_1,x_2,x_3)=(x_1,x_2,x_3,x_0)$).

One round of the standard four partitions Feistel structures is shown in Fig 1.

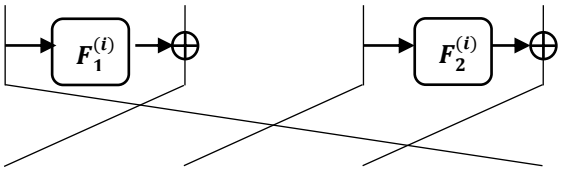

Fig. 1. One round of four partitions Feistel structure

The structure of the standard six partitions structure is shown in Fig 2.

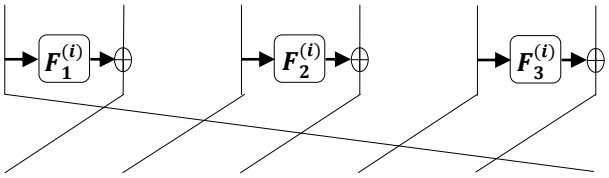

Fig. 2. One round of six partitions Feistel structure

In both structures we assume that each round function is the SP-type F-function which consists of an *mn*-bit round key addition, m *parallel* n-bit bijective S-boxes and an *m***m* matrix with element in GF(2^n).

By relying on switching method instead of using one matrix, we can use multiple matrices. For instance, two matrices are used in Clefia structure. The way of assigning matrices to the functions in Clefia structure is shown in *Fig A.1*. Also the way of assigning matrices to the functions in the proposed four and six partitions structure are respectively shown in *Fig A*.3.

B. Definitions

Active Differential S-box: An S-box which has non-zero input difference [4].

Hamming Weight: Let $\mathbf{x}=(x_0,x_1,...,x_{m-1})$ by $x_i\in\{0,1\}^n$. The Hamming weight $w(\mathbf{x})$ is defined as [1]:

$$w(\mathbf{x})=\#\{i\mid 0\le i\le m-1, x_i\neq 0\} \quad (2)$$

Branch Number: Let P be a linear transformation with m_1 inputs and m_2 outputs. The branch number of P is defined as [1]:

$$Br(P)=\min_{\mathbf{a}\neq 0}\{w(\mathbf{a})+w(P(\mathbf{a}))\} \quad (3)$$

Truncated Difference Vector: Consider a string Δ consisting of m bytes as $\mathbf{\Delta}=(\Delta_0,\Delta_1,...,\Delta_{m-1})$. The truncated difference vector $\mathbf{x}=(x_0,x_1,...,x_{m-1})$ corresponding to $\mathbf{\Delta}$ is defined as [8]:

$$x_i=\begin{cases}0 & if\ \Delta_i=0\\ 1 & otherwise\end{cases} \quad (4)$$

MDS matrix: A matrix with maximum branch number is called MDS. If P is an MDS $m\times m$ matrix, the branch number of P equals to m+1. In the rest of paper we assume that all of the used matrices are MDS.

III. USING MILP IN DIFFERENTIAL ANALYSIS OF FEISTEL STRUCTURE

In MILP, an objective function like $f(x_1,x_2,...,x_n)$ is optimized (minimized or maximized) subject to linear inequalities involving decision variables $x_i, 1\le i\le n$. Therefore to describe MILP program we need to define decision variables, objective function and constraints related to decision variables.

In order to define decision variables to count the active S-boxes of a Feistel structure, consider the F function in the *i*-th round. Suppose that each *n*-bit sequence which is placed at the input of each S-box is corresponded to a binary variable.

Let $x_{i,j}$ denote a truncated variable corresponded to an *n*-bit sequence which is the *j*-th input of F function in the *i*-th round and also the truncated variable $z_{i,j}$ is corresponded to an n-bit sequence which is the *j*-th output of F function in the *i*-th round. A schematic overview of this description is given in Fig. 3.

Therefore the input difference vector of F function will be $(x_{i,0},x_{i,1},...,x_{i,m-1})$ and output difference vector of F function will be $(z_{i,0},z_{i,1},...,z_{i,m-1})$. Now we can describe objective function and constraints related to decision variables.

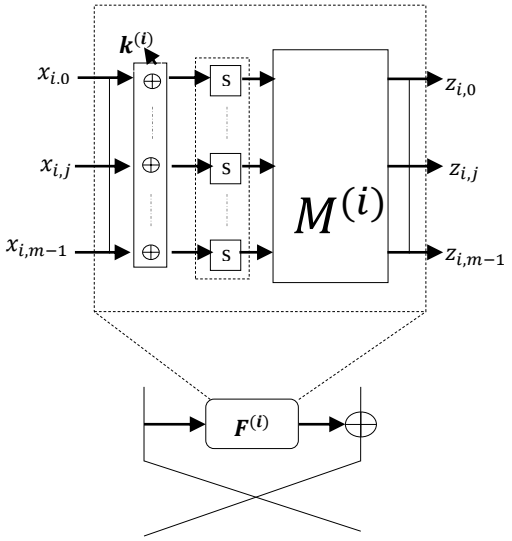

Fig. 3. Binary variables correspond to input and output of each F function in the *i*-th round

A. Equations Describing the XOR Operation

Consider the *i*-th round of Feistel structure for describing XOR operation equations. According to Fig. 4, XOR of each element of corresponding vectors must computed peer to peer.

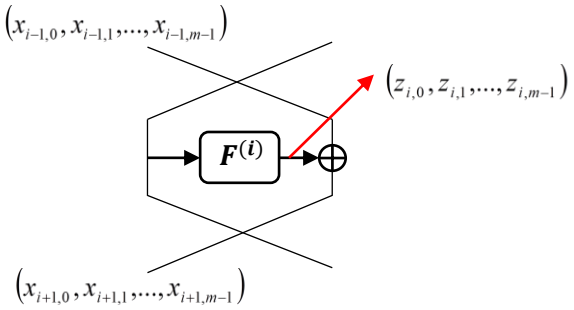

Fig. 4. The difference vector involved in XOR operation in Feistel structure

More precisely the variables $x_{i-1,j}$ and $z_{i,j}$ $(0 \le j \le m-1)$ are input of XOR operation and the variable $x_{i+1,j}$ is the output of XOR operation. It is well known that the branch number of XOR operation is equal to 2. To express this branch number in equations, we need to define a new binary dummy variable for each XOR operation. Therefor we define the binary dummy vector variables $(d_0^i, d_1^i, \ldots, d_{m-1}^i)$. The binary variable d_j^i $(0 \le j \le m-1)$ is zero iff $x_{i-1,j}$ ‘ $z_{i,j}$ and $x_{i+1,j}$ are zero, otherwise it must be equal to one. Thus to describe the relations between input difference vectors and output difference vector, we can write the following inequality:

$$
\begin{aligned}
& x_{i-1,0} + z_{i,0} + x_{i+1,0} \ge 2d_0^i \\
& d_0^i \ge x_{i-1,0} \\
& d_0^i \ge z_{i,0} \\
& d_0^i \ge x_{i+1,0} \\
& x_{i-1,m-1} + z_{i,m-1} + x_{i+1,m-1} \ge 2d_{m-1}^i \\
& d_{m-1}^i \ge x_{i-1,m-1} \\
& d_{m-1}^i \ge z_{i,m-1} \\
& d_{m-1}^i \ge x_{i+1,m-1}
\end{aligned}
\qquad (5)
$$

B. Equations describing F-function

To describe the F function, Fig. 3. According to relation (5), we define the new binary dummy variable called dd^i and assume that the branch number of used matrix is β. Equations (6) are obtained as below:

$$
\begin{aligned}
& x_{i,0} + x_{i,1} + \ldots + x_{i,m-1} + z_{i,0} + z_{i,1} + \ldots + z_{i,m-1} \ge \beta dd^i \\
& dd^i \le \sum_{j=0}^{m-1} x_{i,j} \\
& dd^i \le \sum_{j=0}^{m-1} z_{i,j}
\end{aligned}
\qquad (6)
$$

C. Objective function

The objective function should be defined in a way that number of active S-boxes is minimized. Therefore to obtain the minimum number of active S-boxes of a Feistel structure, we have to minimize sum of all variables which are placed in the input of F function in every round (i.e.,) $\mathbf{min} \sum_{i=0}^{r-1} \sum_{j=0}^{m-1} x_{i,j}$.

To ensure that at least one S-box is active, we add a ..near equation to our MILP program. This linear equation is sum of all truncated binary variables which are corresponded to plaintext. This equation must be greater-equal than one.

II. DIFFERENTIAL ANALYZE OF THE FOUR PARTITIONS FEISTEL STRUCTURE

In this section, the method of counting the minimum number of active S-boxes if explained for four partitions Feistel structure with one MDS matrix (case *A*) and two MDS matrices (case B), by MILP.

It is easy to realize that by generalizing the variables in case *A*, we can calculate the minimum number of active S-boxes of six partitions of Feistel structure with one MDS matrix.

A. Four partitions Feistel structure with one MDS matrix

There are two XOR operations and two F functions in each round of four partitions Feistel structure. We can show the differential behavior of these operations by using the equations which is described in prior section.

To determine the variables which are input and output of the F function, consider first round. We explain the equations for the first round and this process will be repeated for each round and the equations will be added to MILP program until reaching to the round that we want to calculate its minimum number of active S-boxes.

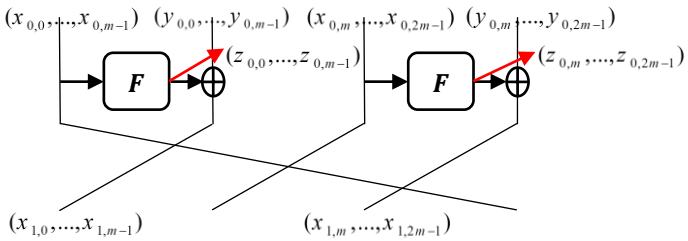

Fig. 5. Deccision variables in round 1 for four partitions Feistel structure

The input difference vectors of F functions are called $(x_{0,0}, \ldots, x_{0,m-1})$ and $(x_{0,m}, \ldots, x_{0,2m-1})$ respectively and also the output difference vectors are called $(z_{0,0}, \ldots, z_{0,m-1})$ and $(z_{0,m}, \ldots, z_{0,2m-1})$ respectively. Also to establish regularity in definition of variables in other rounds, in round one the difference vectors which their XOR with output of F functions must be computed, are called $(y_{0,0}, \ldots, y_{0,m-1})$ and $(y_{0,m}, \ldots, y_{0,2m-1})$ respectively (some parts of plaintext). The output difference vector of XOR operations will be $(x_{1,0}, \ldots, x_{1,m-1})$ and $(x_{1,m}, \ldots, x_{1,2m-1})$ respectively. We continue this process for other rounds.

By defining the binary dummy variables vector $(d_0,...,d_{2m-1})$, the inequalities related to XOR operation for round 1, are similar relation (5).

It is worth noting that we need to define a new binary dummy variables vector for each round. More precisely, every XOR operation needs a new binary dummy variable. Therefore the index of these binary variables must be incremented for the other rounds.

By defining binary dummy variables dd_0 for the left F function and dd_1 for the right F function in round 1, the equations related to F functions in round 1 are obtained as follows:

$$\begin{aligned} &x_{0,0}+...+x_{0,m-1}+z_{0,0}+...+z_{0,m-1}\geq (m+1)dd_0\\ &\sum_{j=0}^{m-1}x_{i,j}+\sum_{j=0}^{m-1}z_{i,j}\geq (m+1)dd_0^i\\ &mdd_0^i\geq \sum_{j=0}^{m-1}x_{i,j}\\ &mdd_0^i\geq \sum_{j=0}^{m-1}z_{i,j} \end{aligned} \tag{7}$$

$$\begin{aligned} &\sum_{j=m}^{2m-1}x_{i,j}+\sum_{j=m}^{2m-1}z_{i,j}\geq (m+1)dd_1^i\\ &mdd_1^i\geq \sum_{j=m}^{2m-1}x_{i,j}\\ &mdd_1^i\geq \sum_{j=m}^{2m-1}z_{i,j} \end{aligned} \tag{8}$$

As before every F-function needs a new binary dummy variable, therefore the index of binary dummy variables must be incremented for other rounds.

According to relations 5, 7 and 8 for one round of four partitions Feistel structure that the branch number of used matrix is m+1 we need $8\times m$ and $4\times m+2$ equations for XOR operations and for F functions respectively. Also to ensure that at least one S-box is active we add equation 9 to our MILP program.

$$\begin{aligned} &(x_{0,0}+...+x_{0,m-1})+(y_{0,0}+...+y_{0,m-1})+\\ &(x_{0,m}+...+x_{0,2m-1})+(y_{0,m}+...+y_{0,2m-1})\geq 1 \end{aligned} \tag{9}$$

The objective function for *r* round is obtained as follows:

$$\min\sum_{i=0}^{r-1}\sum_{j=0}^{2m-1}x_{i,j} \tag{10}$$

B. Clefia structure

The only difference between the Clefia structure and structure in Fig. 5 is the matrices which are used in Clefia structures. These matrices cause the minimum number of active S-boxes will be increased. Therefore to calculate the minimum number of active S-boxes of this structure we have all of relations which we have obtained for prior structure to our MILP program1 and some equations related to the switching method are added to previous non-equalities.

We consider the truncated difference vector $(x_{i,0},...,x_{i,m-1})$ briefly is equivalent to vector $X_{i,0}$ and also $(x_{i,m},...,x_{i,2m-1})$, $(z_{i,0},...,z_{i,m-1})$ and $(z_{i,m},...,z_{i,2m-1})$ are equivalent to $X_{i,1}$, $Z_{i,0}$ and $Z_{i,1}$ respectively. We call the matrix which is used in the first F function M_1 and the matrix in the second F function M_2.

According to *Fig A.1*, some of difference vectors which are involved in the switching mechanism have lied on red and blue path. Thus following relations are obtained respectively:

$$\begin{aligned} X_{0.0}\oplus Z_{1.1}\oplus Z_{3.0}&=X_{4.0}\\ X_{0.1}\oplus Z_{1.0}\oplus Z_{3.1}&=X_{4.1} \end{aligned} \tag{11}$$

According to this point that S-box has no effect on truncated difference vector ($S(X_i)=X_i$), The above relations are equivalent to:

$$\begin{aligned} X_{0.0}\oplus M_2X_{1.1}\oplus M_1X_{3.0}&=X_{4.0}\\ X_{0.1}\oplus M_1X_{1.0}\oplus M_2X_{3.1}&=X_{4.1} \end{aligned} \tag{12}$$

Or:

$$\begin{aligned} [M_1,M_2]\begin{pmatrix}X_{1,1}\\X_{3,0}\end{pmatrix}&=X_{0,0}\oplus X_{4,0}\\ [M_1,M_2]\begin{pmatrix}X_{1,0}\\X_{3,1}\end{pmatrix}&=X_{0,1}\oplus X_{4,1} \end{aligned} \tag{13}$$

According to switching condition that has been explained in [4], If $X_{1,1}\neq \underline{0}\ and\ X_{3,0}\neq \underline{0}$ and also in other relation $X_{1,0}\neq \underline{0}\ and\ X_{3,1}\neq \underline{0}$ the branch number the matrix $[M_1,M_2]$ is equal m+1(the branch number the matrix like $[M_1,M_2]$ must be smaller-equal than branch number of matrices like M_1 or M_2). Inequalities are obtained from (13) as follow:

$$\begin{aligned} \sum_{i=m}^{2m-1}x_{1,i}+\sum_{i=0}^{m-1}x_{3,i}&\geq (m+1)-(\sum_{i=0}^{m-1}x_{0,i}\oplus\sum_{i=0}^{m-1}x_{4,i})\\ \sum_{i=0}^{m-1}x_{1,i}+\sum_{i=m}^{2m-1}x_{3,i}&\geq (m+1)-(\sum_{i=m}^{2m-1}x_{0,i}\oplus\sum_{i=m}^{2m-1}x_{4,i}) \end{aligned} \tag{14}$$

To ensure that the vectors $X_{1,1}\neq \underline{0}\ and\ X_{3,0}\neq \underline{0}$ and also the vectors $X_{1,0}\neq \underline{0}\ and\ X_{3,1}\neq \underline{0}$, we need to define a new binary dummy variable called ddd_0 and ddd_1. Therefor the relations 14 can be written as follows:

$$\begin{aligned} &\sum_{i=0}^{m-1}x_{0,i}+\sum_{i=m}^{2m-1}x_{1,i}+\sum_{i=0}^{m-1}x_{3,i}+\sum_{i=0}^{m-1}x_{4,i}\geq (m+1)ddd_0\\ &ddd_0\leq \sum_{i=m}^{2m-1}x_{1,i}+\sum_{i=0}^{m-1}x_{3,i}\leq 2mddd_0\\ &\sum_{i=m}^{2m-1}x_{0,i}+\sum_{i=0}^{m-1}x_{1,i}+\sum_{i=m}^{2m-1}x_{3,i}+\sum_{i=m}^{2m-1}x_{4,i}\geq (m+1)ddd_1\\ &ddd_1\leq \sum_{i=0}^{m-1}x_{1,i}+\sum_{i=m}^{2m-1}x_{3,i}\leq 2mddd_1 \end{aligned} \tag{15}$$

So the switching condition must be added to MILP program after fifth round and we must obtain relations (15) for every five consecutive round (according to indexes) and we continue this process until reaching the round which we want to calculate its minimum number of active S-boxes.

III. PROPOSED FEISTEL STRUCTURES WITH THREE MDS MATRICES

In this section by relying on simple analyze by using MILP, we have proposed a new standard four partitions and six partitions Feistel structure which both of them are more

resistant against differential cryptanalysis than Clefia structure. In case *A*, we explain about calculating minimum number of active S-boxes of four partitions proposed Feistel structure and in case *B* explain about the six partitions proposed Feistel structure which is generalized state of Clefia.

A. Standard four partitions Feistel structure with three MDS matrices

To analyze this structure, we must add all of the constraints which we have made for Clefia to the MILP program. Since according to Fig.A.2 of *appendix A*, every property which is established for Clefia can be established for this structure even the relations which we have described for switching conditions. The excellence of this structure rather than Clefia is some equations which we have to add to MILP program. According to Fig.A.2, some of difference vectors which are involved in the switching mechanism have lied on red and blue path. Thus following relations are obtained respectively.

$$\begin{aligned} X_{0.0} \oplus Z_{1.1} \oplus Z_{3.0} \oplus Z_{5.1} &= X_{6.1} \\ X_{0.1} \oplus Z_{1.0} \oplus Z_{3.1} \oplus Z_{5.0} &= X_{6.0} \end{aligned} \tag{16}$$

By similar method to obtain relations (15), the relations (16) are equivalent to relations (17) with this difference that In this case we don't need to define new binary dummy variables because it isn't possible that the sum of elements of three truncated difference vectors $X_{1,1}$ *and* $X_{3,0}$ *and* $X_{5,1}$ and also $X_{1,0}$ *and* $X_{3,1}$ *and* $X_{5,0}$ be zero at the same time. It is mentioned for more specific case with two truncated difference vector before.

$$\begin{aligned} &\sum_{i=0}^{m-1} x_{0,i} + \sum_{i=m}^{2m-1} x_{1,i} + \sum_{i=0}^{m-1} x_{3,i} + \sum_{i=m}^{2m-1} x_{5,i} + \sum_{i=m}^{2m-1} x_{6,i} \geq (m+1) \\ &\sum_{i=m}^{2m-1} x_{0,i} + \sum_{i=0}^{m-1} x_{1,i} + \sum_{i=m}^{2m-1} x_{3,i} + \sum_{i=0}^{m-1} x_{5,i} + \sum_{i=0}^{m-1} x_{6,i} \geq (m+1) \end{aligned} \tag{17}$$

Relation (17) must be obtained for every six consecutive round and we continue this process until the round which we want to calculate its minimum number of active S-boxes. We add the obtained equations to our MILP program.

B. Generalizing Clefia in to Standard six partitions Feistel structure with three MDS matrices

Generalizing Clefia in to Standard six partitions Feistel structure with three MDS matrices As we mentioned in Section *IV* to analyze this structure with one MDS matrix we must generalize the variables of four partitions to six partitions. So the objective function for *r* round will be as

$$\min \sum_{i=0}^{r-1} \sum_{j=0}^{3m-1} x_{i,j} \,. \tag{18}$$

Now after adding XOR and F-functions relations to our MILP program to obtain the equations of switching method we follow the same process which we have done for clefia structure. In *Fig.3 of appendix A*, the way of assigning matrices to F-functions are shown and some of difference vectors which are involved in the switching mechanism have lied on red and blue and green path. So the following relations are obtained for the red, blue and green path respectively:

TABEL I.
COMPARING MINIMUM NUMBER OF ACTIVE S-BOXES FOR THREE FOUR PARTITIONS AND TWO SIX PARTITIONS FEISTEL STRUCTURE

round	*GFS4 With 1 matrix*	*Clefia With 2 matrices*	*GFS4 With 3 matrices*	*GFS6 With 1 matrix*	*GFS6 With 3 matrices*
1	0	0	0	0	0
2	1	1	1	1	1
3	2	2	2	2	2
4	6	6	6	6	6
5	8	8	8	8	8
6	12	12	12	12	12
7	12	14	16	14	14
8	13	18	18	18	18
9	14	20	20	21	21
10	18	22	23	25	25
11	20	24	26	27	28
12	24	28	30	30	34
13	24	30	32	31	37
14	25	34	35	35	38
15	26	36	37	37	42
16	30	38	40	41	44
17	32	40	42	43	48
18	36	44	46	47	50
19	36	46	48	50	54
20	37	50	51	54	57
21	38	52	53	56	61
22	42	55	56	59	64
23	44	56	58	60	69
24	48	59	62	64	73
25	48	62	64	66	74
26	49	65	67	70	78

$$\begin{aligned} X_{0.0} \oplus Z_{1.2} \oplus Z_{3.1} \oplus Z_{5.0} &= X_{6.0} \\ X_{0.1} \oplus Z_{1.0} \oplus Z_{3.2} \oplus Z_{5.1} &= X_{6.1} \\ X_{0.2} \oplus Z_{1.1} \oplus Z_{3.0} \oplus Z_{5.2} &= X_{6.2} \end{aligned} \tag{19}$$

Finally By similar method to obtain relations 15, we have:

$$\begin{aligned} &\sum_{i=0}^{m-1} x_{0,i} + \sum_{i=2m}^{3m-1} x_{1,i} + \sum_{i=m}^{2m-1} x_{3,i} + \sum_{i=0}^{m-1} x_{5,i} + \sum_{i=0}^{m-1} x_{6,i} \geq (m+1)ddd_0 \\ &ddd_0 \leq \sum_{i=2m}^{3m-1} x_{1,i} + \sum_{i=m}^{2m-1} x_{3,i} + \sum_{i=0}^{m-1} x_{5,i} \leq 3mddd_0 \\ &\sum_{i=m}^{2m-1} x_{0,i} + \sum_{i=0}^{m-1} x_{1,i} + \sum_{i=2m}^{3m-1} x_{3,i} + \sum_{i=m}^{2m-1} x_{5,i} + \sum_{i=m}^{2m-1} x_{6,i} \geq (m+1)ddd_1 \\ &ddd_1 \leq \sum_{i=0}^{m-1} x_{1,i} + \sum_{i=2m}^{3m-1} x_{3,i} + \sum_{i=m}^{2m-1} x_{5,i} \leq 3mddd_1 \\ &\sum_{i=2m}^{3m-1} x_{0,i} + \sum_{i=m}^{2m-1} x_{1,i} + \sum_{i=0}^{m-1} x_{3,i} + \sum_{i=2m}^{3m-1} x_{5,i} + \sum_{i=2m}^{3m-1} x_{6,i} \geq (m+1)ddd_2 \\ &ddd_2 \leq \sum_{i=m}^{2m-1} x_{1,i} + \sum_{i=0}^{m-1} x_{3,i} + \sum_{i=2m}^{3m-1} x_{5,i} \leq 3mddd_2 \end{aligned} \tag{20}$$

Similar to Clefia relations, we must consecutively obtain relation (20) for every seven consecutive round and continue this process until reaching the round which we want to calculate its minimum number of active S-boxes.

In Table 1, we have shown the minimum number of active S-boxes of three standard four partitions Feistel structure (with one and two and three MDS matrices) and also 2 standard six-partitions Feistel structure (with one and three MDS matrices) for 26 rounds with branch number 5 .

Also, Table 1 shows that the proposed four and six partitions Feistel structure with three MDS matrices are more resistant against the differential cryptanalysis rather than Clefia structure. It is clear that we can expect similar results for linear cryptanalysis. In this paper we used CPLEX software to obtain results.

REFERENCES

[1] K. Shibutani, "On the diffusion of generalized feistel structures regarding differential and linear cryptanalysis" Selected Areas in Cryptography, pp. 211-228, 2010.

[2] T. Shirai, K. Araki, "On generalized Feistel structures using the diffusion switching mechanism", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, pp . 2120-2129, 2008.

[3] S. Wu, M. Wang," Security Evaluation against Differential Cryptanalysis for Block Cipher Structures", IACR Cryptology ePrint Archive, 2011.

[4] T. Shirai, K. Shibutani, "Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices", Fast Software Encryption, pp. 260-278, 2004.

[5] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata," The 128-bit blockcipher CLEFIA", Fast software encryption, pp. 181-195, 2007.

[6] Q. Wang, A. Bogdanov, "The provable constructive effect of diffusion switching mechanism in CLEFIA-type block ciphers", Information Processing Letters, pp. 427-432, 2011.

[7] T. Shirai, B. Preneel, "On Feistel ciphers using optimal diffusion mappings across multiple rounds", Springer, pp. 1-15, 2004.

[8] N. Mouha, Q. Wang, D. Gu, B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming", Information Security and Cryptology, pp. 57-76, 2011.

[9] D. Watanabe, K. Okamoto, T. Kaneko, "A hardware-oriented light weight pseudo-random number generator enocoro-128v2", The Symposium on Cryptography and Information Security. pp. 3D1–3, 2010.

[10] IBM: IBM ILOG CPLEX Optimizer. http://www .ibm. com /software/integration/optimization/cplex-optimizer/.

[11] A. Bogdanov, K. Shibutani, "Generalized Feistel networks revisited", Designs, codes and cryptography, pp. 75-97, 2013.

Appendix A. The way of assigning matrices to the functions in Clefia and proposed structures

Fig A.1. Clefia structure with 2 MDS matrices and the difference vector involved in switching path

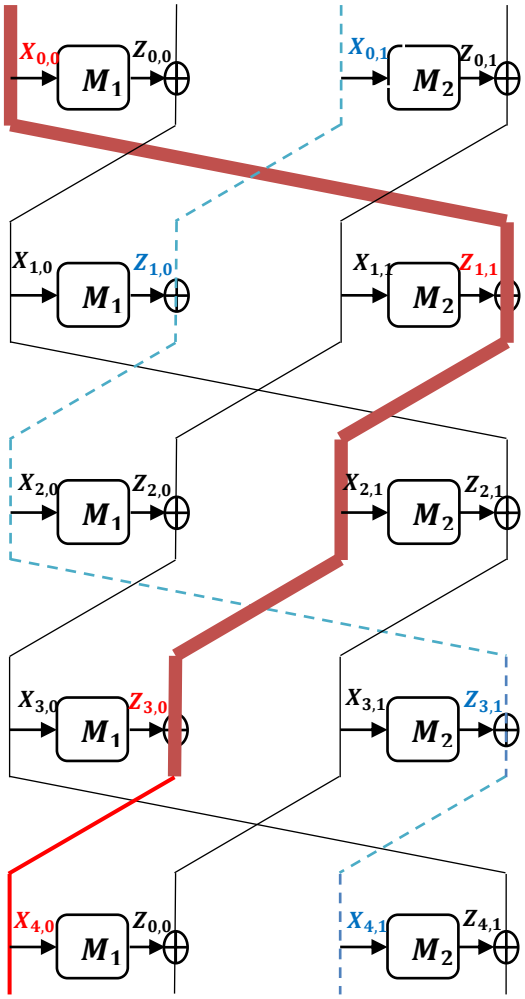

Fig. A.2. Four partitions structure with 3 MDS matrices and the difference vector involved in switching path

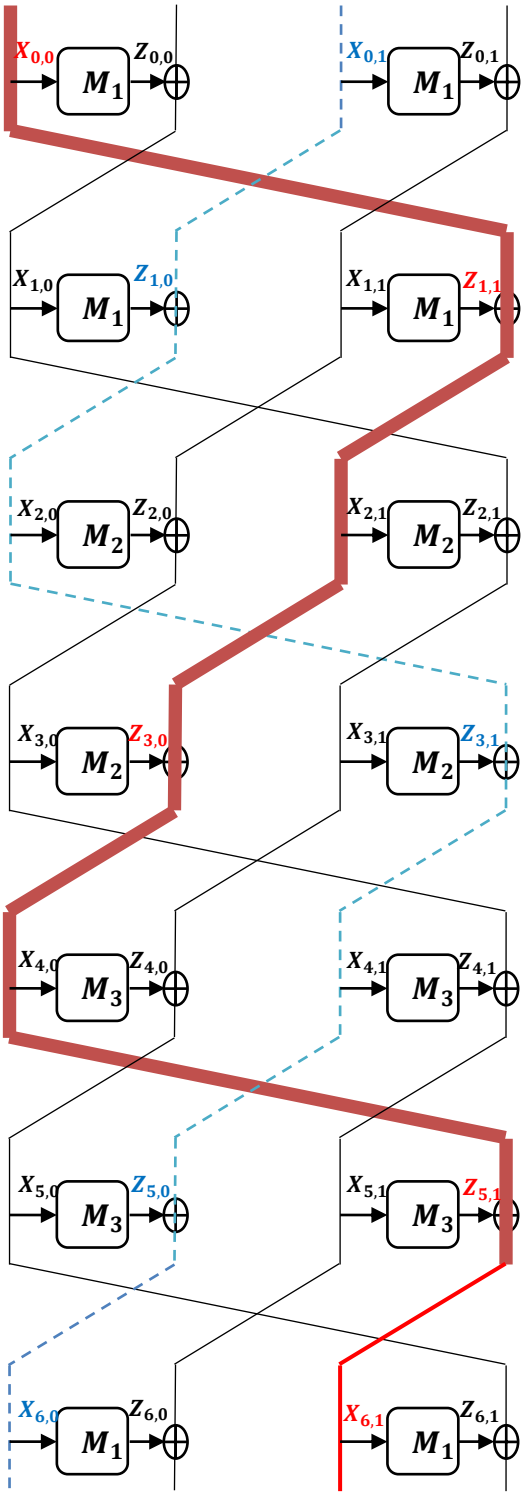

Fig. A.3. Six partitions structure with 3 MDS matrices and the difference vector involved in switching path