Using MILP in Analysis of Feistel Structures and Improving Type II GFS by Switching Mechanism

Mahdi Sajadieh and Mohammad Vaziri

[1] Department of Electrical Engineering , Khorasgan Branch , Islamic Azad University, Isfahan, Iran
[2] Department of Mathematics, Iran University of Science and Technology (IUST), Tehran, Iran
m.sajadieh@khuisf.ac.ir,
mohammad.vaziri67@gmail.com,

Abstract. Some features of Feistel structures have caused them to be considered as an efficient structure for design of block ciphers. Although several structures are proposed relied on Feistel structure, the type-II generalized Feistel structures (GFS) based on SP-functions are more prominent. Because of difference cancellation, which occurs in Feistel structures, their resistance against differential and linear attack is not as expected. Hitherto, to improve the immunity of Feistel structures against differential and linear attack, two methods are proposed. One of them is using multiple MDS matrices, and the other is using changing permutations of sub-blocks.

In this paper by using MILP and summation representation method, a technique to count the active S-boxes is proposed. Moreover in some cases, the results proposed by Shibutani at SAC 2010 are improved. Also multiple MDS matrices are applied to GFS, and by relying on a new proposed approach, the new inequalities related to using multiple MDS matrices are extracted, and results of using the multiple MDS matrices in type II GFS are evaluated. Finally results related to linear cryptanalysis are presented. Our results show that using multiple MDS matrices leads to 22% and 19% improvement in differential cryptanalysis of standard and improved 8 sub-blocks structures, respectively, after 18 rounds.

Keywords: MILP, Generalized Feistel structure, Switching mechanism, Differential cryptanalysis, Linear cryptanalysis.

1 Introduction

Nowadays, security is one of the most important components of information transition, and cryptography is inseparable part of security. Block ciphers are one of the most important tools, which are used in cryptography. These ciphers must be resistant against the existing security cryptanalysis that the most important of them are differential and linear cryptanalysis.

Feistel structures are significant category of block ciphers, which have been under several evaluation so far. Perhaps CAMELLIA [1] and CLEFIA [12] are the most important block ciphers that are designed based on these structures. The CLEFIA block cipher uses four sub-blocks Feistel structure with switching mechanism [10]. In switching mechanism multiple MDS matrices with specified properties are used. Using switching mechanism in CLEFIA provides *1.3* times more active S-boxes rather than the structure with one matrix. Also as mentioned in [10, 11], for two sub-blocks Feistel structure with multiple MDS matrices, the total number of active S-boxes are *1.2* times more than two sub-blocks Feistel structure with one MDS matrix.

Hitherto, a lot of method have been proposed to count the number of active S-boxes of Feistel structures. The first method for Feistel structures with SPN round functions is proposed in [4]. This method is able to offer a lower bound for the number of differential and linear active S-boxes with branch number β. In [9], a method is proposed to calculate the minimum number of active S-boxes of block cipher Camellia, and the existing bound is improved for this block cipher. Also in [13, 7], the number of active S-boxes is obtained by changing the standard method, and proposing a particular algorithm. Although employing multiple MDS matrices in GFS are discussed in [3, 8], accurate results are not reported.

Probably, using linear programming method in calculating the number of active S-boxes of block ciphers is one of the most important exciting methods. This method is discussed in several papers such as [2, 5]. In order to evaluate word-oriented block ciphers, however, a comprehensive method is proposed in [5]. Also in [6] due to have better performance from the features of MDS matrices, a method is proposed.

In this paper by using linear programming and the proposed idea in [6], first a new method to count the number of differential and linear active S-boxes in Feistel structures is presented, and the obtained results are compared with results in [7]. Other major contribution of the paper is referring to inequalities that are extracted from imposing switching mechanism, and results that are obtained by imposing switching mechanism on generalized Feistel structures are presented. Moreover, the results for the best 8 sub-blocks Feistel structures that employ 2 and 4 multiple MDS matrices are reported. Based on our researchs, the results of using $\frac{l}{4}$ MDS matrices and $\frac{l}{2}$ MDS matrices in differential cryptanalysis of l sub-blocks structures, are fairly close. Finally we analyze the switching mechanism in linear attack. As far as we know, an accurate method for cryptanalyzing the switching mechanism is not proposed so far. Instead, our method represents the accurate cryptanalysis for switching mechanism.

The rest of paper is organized as follows. In Sect.2 we review the details of GFS structures, and explain about summation representation, which is used in our MILP method. In Sect.3 first we present our method to calculate the minimum number of differential active S-boxes of *2* sub-blocks Feistel structures, and we generalize this method for structures with more number of sub-blocks. In Sect.4 inequalities which describe switching mechanism are proposed, and in the following in term of number of active S-boxes, the best generalized Feistel structures are introduced. In Sect. 5 by expanding the proposed method, linear cryptanalysis is evaluated. Finally, we conclude in Sect. 6.

2 Preliminaries

In this section we clarify that what type of Feistel structures exactly we aim to evaluate, and point out that what is the difference between our method and well known MILP method, which is proposed in [5].

2.1 GFS Structures

In GFS, a plaintext is divided to l sub-blocks, where l is an even integer. if $(X_0, X_1, ..., X_{l-1})$ represents the l divided sub-blocks of a state, a single round of l sub-blocks GFS follows a permutation over $(\{0,1\}^{mn})^l$ as:

$$(X_0, X_1, ..., X_{l-1}) \rightarrow \pi(X_0, F_0(X_0) \oplus X_1, X_2, F_1(X_2) \oplus X_3, ..., F_{(l-2)/2}(X_0) \oplus X_1) \tag{1}$$

In relation (1) $F_i : \{0,1\}^{mn} \rightarrow \{0,1\}^{mn}$ is the i-th round function, and $\pi : (\{0,1\}^{mn})^l \rightarrow (\{0,1\}^{mn})^l$ is a deterministic permutation over l sub-blocks. Throughout the paper, we consider each round function is SP-function, and each sub-block is consisted of n S-boxes with size of m bits. Therefore, it is easy to verify that a GFS with l sub-blocks is an lmn bit block cipher.

In this paper we assume that π is a word-based permutation. In the rest of the paper, GFS_l^{std} is interpretted as a standard type-II GFS with l sub-blocks, where $\pi(X_0, X_1, ..., X_{l-1}) = (X_1, X_2, ..., X_{l-1}, X_0)$, and GFS_l^{imp} is interpretted as an improved type-II GFS with l sub-blocks as pointed out by the authors of [13]. For instance, the permutation in $GFS_6^{imp}(No.1)$ is as $\pi(X_0, X_1, ..., X_5) = (X_3, X_0, X_1, X_4, X_5, X_2)$, and the permutation in $GFS_8^{imp}(No.1)$, which is one of the most important evaluated structures in this paper, is as $\pi(X_0, X_1, ..., X_7) = (X_3, X_0, X_1, X_4, X_7, X_2, X_5, X_6)$.

2.2 Summation Representation

As mentioned above, each round function in GFS contains an mn bit block as an input, and each bijective S-box is m bits (n parallel m bit S-boxes), and also $\mathbf{P}$ is an $n \times n$ matrix with m bit elements, where we assume that β is branch number of this matrix. In order to count the number of active S-boxes, the truncated method is used. Therefore, in this case, the S-box does not have any effect on truncated difference or mask. Because of using branch number, the place of elements does not care to be zero or not, and just the number of them is important. Hence for every n truncated vector bits, the summation of elements of that vector are allocated (i.e. we replace an integer number between *0* to n instead of a vector with size of n). From now on, we call this method "summation representation" [6]. We emphasize that in summation representation, 2^n possible representation reduces to $n+1$ possible representation. For instance, in relation (2) the truncated representation and summation representation are shown for a vector as an input of F-function with 4 8-bit elements:

$$\begin{pmatrix} 6 \\ 15 \\ 0 \\ 158 \end{pmatrix} \xrightarrow{truncated} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \xrightarrow{summation} 3 \qquad (2)$$

In [5], due to count the differential and linear active S-boxes of word-oriented block ciphers, the truncated method is used. In contrast, we use summation method to count the differential and linear active S-boxes of word-oriented block ciphers. Throughout this paper all of the inputs and outputs are shown in a summation representation. It is worth mentioning that, our method can be apllied for both structures with MDS and non MDS matrices. However we prefer to describe the inequalities, by considering the fact that all of applied matrices be MDS.

3 Counting the Differential Active S-boxes

In cryptanalysis of Feistel structure (two sub-blocks or multiple sub-blocks) with an SP-functions, we deal with two functions. One of them is SP-function and the other is XOR function.

Hearafter, summation representation of a difference vector "$\mathbf{x}$" is denoted by "x^c", where "x^c" is the number of non zero elements of "$\mathbf{x}$" shows the results for.

Equations Describing the SP-Function. According to Figure 1, assume that input and output of the i-th SP-function are x_i^c and z_i^c, respectively, where both of them are an integer number between 0 to n.

The branch number of matrix $\mathbf{P}$ is β. Therefore, we have:

$$\begin{cases} z_i^c = 0 & \text{if } x_i^c = 0 \\ x_i^c + z_i^c \geq \beta & \text{otherwise} \end{cases} \qquad (3)$$

The function is conditional. Considering [5], we need to introduce a new binary dummy variable b_i to convert the condition into inequality, where $b_i \in \{0,1\}$. Then we have:

$$\begin{cases} x_i^c + z_i^c \geq \beta b_i \\ b_i \leq x_i^c \leq n b_i \\ b_i \leq z_i^c \leq n b_i \end{cases} . \qquad (4)$$

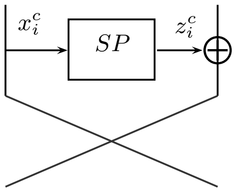

Fig. 1. Summation variables related to the SP-function of Feistel structure

Note that we assumed that an employed matrix be MDS, and this leads to $\beta = n + 1$. In this case if x_i^c be nonzero, certainly z_i^c is nonzero, since the maximum amount of x_i^c is n, and $x_i^c + z_i^c \geq n + 1$ causes that $z_i^c \geq 1$. Therefore inequality $b_i \leq z_i^c$ is redundant and it could be eliminated. As a rule, for an SP-function, inequalities are turned as follows:

$$\begin{cases} 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \\ x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ z_i^c \leq nb_i \end{cases} \tag{5}$$

Equations Describing the XOR operation. For describing the XOR operation consider Figure 2. To evaluate XOR operation in summation structure, regard to $\mathbf{y_i} = \mathbf{x_i} \oplus \mathbf{z_i}$, it is clear that the maximum amount of y_i^c is equal to summation of two inputs. Also the minimum amount of y_i^c won't be less than subtract of absolute value of two inputs.

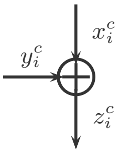

Fig. 2. Summation variables related to XOR operation of Feistel structure

For instance, if x_i^c and z_i^c are equal to *3* and *1*, respectively, the maximum amount that z_i^c can eliminate from *3* nonzero elements of x_i^c is *1*, and the minimum amount of y_i^c will be *2*. Also in best case z_i^c is nonzero in a place that x_i^c is zero and in this case the result of XOR has *4* nonzero elements. Under this notation, for converting XOR relation in to Inequality, the following three Inequalities are obtained:

$$\begin{cases} x_i^c + z_i^c \geq y_i^c \\ \|x_i^c - z_i^c\| \leq y_i^c \end{cases} \Longrightarrow \begin{cases} x_i^c + z_i^c \geq y_i^c \\ x_i^c - z_i^c \leq y_i^c \\ z_i^c - x_i^c \leq y_i^c \end{cases} \tag{6}$$

Therefore, for each round of Feistel structure with an SP-type F-function, where matrix **P** be an MDS matrix, we need *4* variables and *11* inequalities. More precisely 8 inequalities are derived from SP-function, and 3 inequalities are derived from XOR operation. Needless to say, if we wanted to describe such a structure, which contains n S-boxes in its F-functions, with prior well known MILP model, we needed to define $4n$ variables. Also $2n+1$ inequalities are needed to describe the SP-function, and $4n$ inequalities was needed to describe the XOR operation. Besides that, we need just *1* binary dummy variable for SP-function in our model, whereas we need *1* and n binary dummy variables for SP-function and XOR operation in prior model, respectively.

We know that, counting the number of nonzero inputs of SP-functions is equivalent to count the number of active S-boxes. According to the way of defining variables in our method, x_i variable denotes the number of active S-boxes in the i-th SP-function. Therefore, to calculate the minimum number of active S-boxes, the summation of x_i variables must be minimized.

3.1 Evaluating Two Sub-Blocks Feistel Structure

Figure 3 shows the details of two sub-blocks Feistel structure that is started from the first round.

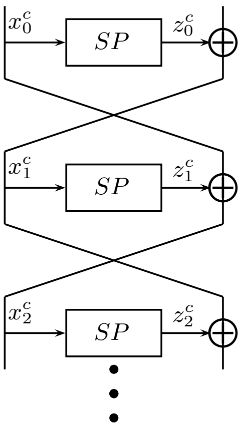

Fig. 3. The way of defining summation variables in two sub-blocks Feistel structure

According to indices of variables in Figure 3, and inequalities (5) and (6), for each round with an MDS matrix we have:

$$\begin{cases} 0 \le x_i^c \le n \\ 0 \le z_i^c \le n \\ x_i^c + z_i^c \ge (n+1)b_i \\ b_i \le x_i^c \le nb_i \\ z_i^c \le nb_i \end{cases} \qquad and \qquad (for\ i \ge 1) \begin{cases} x_{i-2}^c + z_{i-1}^c \ge x_i^c \\ x_{i-2}^c - z_{i-1}^c \le x_i^c \\ z_{i-1}^c - x_{i-2}^c \le x_i^c \end{cases} \qquad (7)$$

It is worth noting that, the variable corresponded to plain text $(x_{-1}^c + x_0^c)$ must be nonzero. Thus the inequality $x_{-1}^c + x_0^c \ge 1$ must be added. Finally by organizing inequalities system and calculating the minimum amount of $\sum_{j=0}^{n-1} x_j^c$ and solving it by IBM-CPLEX, the minimum number of active S-boxes for $n = 4$ and $n = 8$ for r rounds with branch number β are obtained as $\lfloor \frac{r}{4} \rfloor (\beta + 1) + (r) mod 4 - 1$. Table 1 shows the results for two sub-blocks Feistel with $n = 4$ and $n = 8$ and $\beta = n + 1$.

Table 1. Minimum number of active S-boxes of two sub-blocks Feistel

round	Feistel with n=4	Feistel with n=8
1	0	0
2	1	1
3	2	2
4	5	9
5	6	10
6	7	11
7	8	12
8	11	19
9	12	20
10	13	21
11	14	22
12	17	29
13	18	30
14	19	31
15	20	32
16	23	39
17	24	40
18	25	41

3.2 Evaluating Generalized Feistel Structures

The process that has described for two sub-blocks Feistel structure can be expanded to type I and type II GFS. In the following the inequalities are described for GFS_8^{std}. Figure 4 shows summation variables for the first three rounds of GFS_8^{std}.

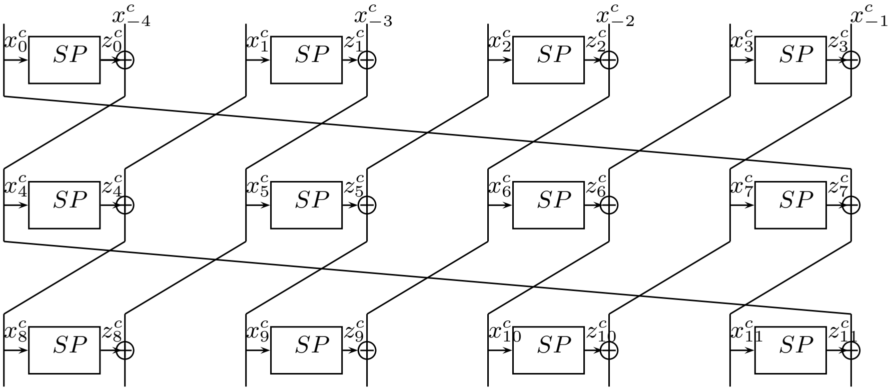

Fig. 4. The way of defining summation variables in standard eight sub-blocks Feistel structure

According to the above rules, GFS_8^{std} is subjected to:

$$\begin{cases} 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \\ x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ z_i^c \leq nb_i \end{cases} \tag{8}$$

$$(for\ 4 \leq i \leq 7) \begin{cases} x^c_{i-8} + z^c_{i-4} \geq x_i^c \\ x^c_{i-8} - z^c_{i-4} \leq x_i^c \\ z^c_{i-8} - x^c_{i-4} \leq x_i^c \end{cases} (for\ i \geq 8) \begin{cases} x^c_{i-8+(i+1)mod4-(i)mod4} + z^c_{i-4} \geq x_i \\ x^c_{i-8+(i+1)mod4-(i)mod4} - z^c_{i-4} \leq x_i^c \\ z^c_{i-4} - x^c_{i-8+(i+1)mod4-(i)mod4} \leq x_i^c \end{cases} \tag{9}$$

Our results for $n = 4$ are summarized for standard and improved generalized Feistel structures from $l = 4$ sub-blocks till $l = 16$ sub-blocks in Table 2 and 3, respectively. In these tables results are compared with [7]. In these tables our different results are bold.

Table 2. The Minimum Number of Active S-boxes in GFS_l^{std} with n=4, the columns marked by ”*” are our results

	GFS_4^{std}		GFS_6^{std}		GFS_8^{std}		GFS_{10}^{std}		GFS_{12}^{std}		GFS_{14}^{std}		GFS_{16}^{std}	
round	*	[7]	*	[7]	*	[7]	*	[7]	*	[7]	*	[7]	*	[7]
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
4	6	6	6	6	6	6	6	6	6	6	6	6	6	6
5	8	8	8	8	8	8	8	8	8	8	8	8	8	8
6	12	12	12	12	12	12	12	12	12	12	12	12	12	12
7	12	12	14	14	14	14	14	14	14	14	14	14	14	14
8	13	13	18	18	18	18	18	18	18	18	18	18	18	18
9	14	14	21	21	21	21	21	21	21	21	21	21	21	21
10	18	18	25	25	25	25	25	25	25	25	25	25	25	25
11	20	20	27	27	28	28	28	28	28	28	28	28	28	28
12	24	24	30	30	36	36	36	36	36	36	36	36	36	36
13	24	24	31	31	36	36	39	39	39	39	39	39	39	39
14	25	25	35	35	37	37	43	43	43	43	43	43	43	43
15	26	26	37	37	38	38	47	47	47	47	47	47	47	47
16	30	30	41	41	42	42	54	54	54	54	54	54	54	54
17	32	32	43	43	44	44	58	58	58	58	58	58	52	52
18	36	36	47	47	48	48	**62**	58	62	62	62	62	62	62

Table 3. The Minimum Number of Active S-boxes in GFS_l^{imp} with n=4, the columns marked by ”*” are our results

	GFS_6^{imp}		GFS_8^{imp}		GFS_{10}^{imp}		GFS_{12}^{imp}		GFS_{14}^{imp}		GFS_{16}^{imp}	
round	*	[7]	*	[7]	*	[7]	*	[7]	*	[7]	*	[7]
1	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2	2	2	2	2
4	6	6	6	6	6	6	6	6	6	6	6	6
5	8	8	8	8	8	8	8	8	8	8	8	8
6	12	12	12	12	12	12	12	12	12	12	12	12
7	14	14	14	14	14	14	14	14	14	14	14	14
8	**23**	22	23	23	**26**	23	18	18	**26**	23	**26**	23
9	24	24	26	26	29	29	21	21	29	29	31	31
10	26	26	29	29	**35**	34	29	29	37	37	**43**	40
11	28	28	32	32	36	36	32	32	40	40	48	48
12	32	32	39	39	**43**	45	**42**	39	**52**	49	**57**	54
13	**34**	33	**42**	40	44	44	45	45	54	54	60	60
14	38	38	**45**	44	48	48	**54**	53	**64**	60	**66**	63
15	40	40	46	46	50	50	57	57	**66**	63	**69**	70
16	**48**	46	50	50	54	54	**61**	60	**77**	71	76	76
17	48	48	52	52	56	56	64	64	**82**	76	78	78
18	50	50	56	56	**68**	65	**70**	68	**84**	83	87	87

4 Evaluating Switching Mechanism

In switching mechanism instead of using one matrix, multiple matrices are used in a way that the number of differential and linear active S-boxes will be significantly more than the case of using one matrix. In this section, at first inequalities related to switching properties for two sub-blocks structure are described, and then for four sub-blocks. Finally inequalities for six and eight sub-blocks structure are listed.

In Figure 5 switching mechanism is imposed on two sub-blocks Feistel structure. In this structure, two MDS matrices $\mathbf{M_1}$ and $\mathbf{M_2}$ are used, where the branch number of matrix $\left[\mathbf{M_1}\ \mathbf{M_2}\right]_{n\times 2n}$ is $n+1$. In order to count the number of active S-boxes of this block cipher, some inequalities must be added to prior corresponded model, which has only one matrix in its structure.

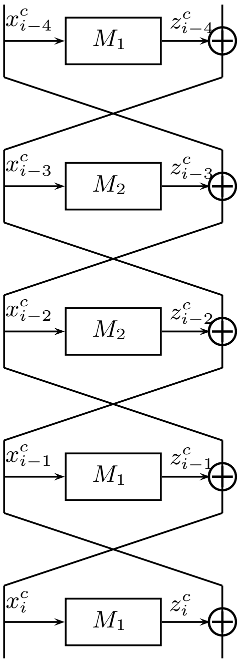

Fig. 5. The way of defining summation variables in two sub-blocks Feistel structure, imposed by switching mechanism

According to Figure 5, relations between inputs and outputs of five consecutive rounds are as follows:

$$\begin{cases} \mathbf{x_i} = \mathbf{z_{i-1}} \oplus \mathbf{x_{i-2}} \\ \mathbf{x_{i-2}} = \mathbf{z_{i-3}} \oplus \mathbf{x_{i-4}} \end{cases} \implies \quad \mathbf{x_i} = \mathbf{z_{i-1}} \oplus \mathbf{z_{i-3}} \oplus \mathbf{x_{i-4}} \tag{10}$$

More precisely, according to effect of S-box on truncated method, above relation can described as follows:

$$\begin{bmatrix}\mathbf{M_1}\ \mathbf{M_2}\end{bmatrix} \begin{bmatrix}\mathbf{x_{i-1}} \\ \mathbf{x_{i-3}}\end{bmatrix} = \mathbf{x_i} \oplus \mathbf{x_{i-4}} \quad or \quad \begin{bmatrix}\mathbf{M_2}\ \mathbf{M_1}\end{bmatrix} \begin{bmatrix}\mathbf{x_{i-1}} \\ \mathbf{x_{i-3}}\end{bmatrix} = \mathbf{x_i} \oplus \mathbf{x_{i-4}} \tag{11}$$

Now converting switching mechanism into inequalities contains two steps: the first step refers to the way of interpreting the relation (10), and the second step refers to guaranteeing at least one of amounts $\mathbf{x_{i-1}}$ and $\mathbf{x_{i-3}}$ must be nonzero. In the following, the above two steps are elaborated, respectively.

Firstly, according to feature of switching, the matrix $\begin{bmatrix}\mathbf{M_1}\ \mathbf{M_2}\end{bmatrix}_{n\times 2n}$ has branch number $n+1$. Thus, if in a relation $\begin{bmatrix}\mathbf{M_1}\ \mathbf{M_2}\end{bmatrix} \begin{bmatrix}\mathbf{a} \\ \mathbf{b}\end{bmatrix} = \mathbf{c} \oplus \mathbf{d}$, at least one of amounts $\mathbf{a}$ and $\mathbf{b}$ be nonzero, the relation $a^c + b^c + c^c + d^c \geq n+1$ is established. To be more specific, $a^c + b^c + \|\mathbf{c} \oplus \mathbf{d}\| \geq n+1$ is correct, and since it is easy to verify that $c^c + d^c \geq \|\mathbf{c} \oplus \mathbf{d}\|$, consequently the relation is described as mentioned. It is remarkable that, this relation corresponds with proposed lemmatta in [11]. If all the variables a^c, b^c, c^c, d^c be zero, a paradox occurs in the inequlity. In order to avoid this paradox, a new binary dummy variable is needed to define.

Secondly, at least one of amounts $\mathbf{a}$ and $\mathbf{b}$ are supposed to be nonzero. Towards this end, the addition of a^c and b^c must be grater-equal than 1. Also, it is obvious that the addition of a^c and b^c is not more than $2n$. As a result, the relation $1 \leq a^c + b^c \leq 2n$ is attained. It is easy to verify that the paradox in prior step is appeared again. In order to overcome the aforementioned problem, the same dummy variable, which is defined in previous step, is used.

With all these taken to account, by defining the new binary dummy variable called bb_i, the description of switching properties for five consecutive rounds of two sub-blocks Feistel structure is as follows:

$$\begin{aligned} x_i^c + x_{i-1}^c + x_{i-3}^c + x_{i-4}^c \geq (n+1)bb_i \\ bb_i \leq x_{i-1}^c + x_{i-3}^c \leq 2nbb_i \end{aligned} \tag{12}$$

Therefore, for the fifth round to next, for each five consecutive rounds, inequalities related to switching mechanism must be added.

Figure 6 shows the structure of four sub-blocks type II GFS (CLEFIA), which two matrices $\mathbf{M_1}$ and $\mathbf{M_2}$ are used in it:

As mentioned above, in CLEFIA two MDS matrices are used. Patterning the process that was done for two sub-blocks structure, for adding inequalities

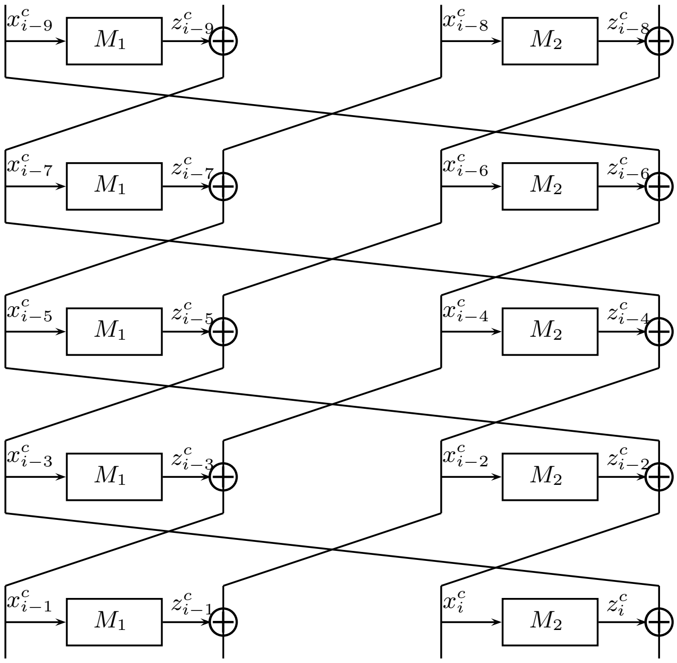

Fig. 6. The way of defining summation variables in CLEFIA

related to switching mechanism, relation between inputs and outputs of five consecutive round is as follows:

$$\begin{cases} \mathbf{x_{i-1}} = \mathbf{z_{i-3}} \oplus \mathbf{z_{i-6}} \oplus \mathbf{x_{i-9}} \\ \mathbf{x_i} = \mathbf{z_{i-2}} \oplus \mathbf{z_{i-7}} \oplus \mathbf{x_{i-8}} \end{cases} \tag{13}$$

By following the same process which was done for two sub-blocks structure, we have:

$$\begin{aligned} x_{i-1}^c + x_{i-3}^c + x_{i-6}^c + x_{i-9}^c \geq (n+1)bb_{i-1} \\ bb_{i-1} \leq x_{i-3}^c + x_{i-6}^c \leq 2nbb_{i-1} \\ \\ x_i^c + x_{i-2}^c + x_{i-7}^c + x_{i-8}^c \geq (n+1)bb_i \\ bb_i \leq x_{i-2}^c + x_{i-7}^c \leq 2nbb_i \end{aligned} \tag{14}$$

Therefore, for the fifth round to next, for each five consecutive rounds, switching feature must be added. We stress that, the obtained results exactly match with [12].

In six sub-blocks type II GFS which consists of standard and improved structure [13], in order to have the best performance, three MDS matrices $\mathbf{M_1}$, $\mathbf{M_2}$

and $\mathbf{M_3}$ must be used. More matrices have not considerable influence. Inequalities that are obtained for switching feature in GFS_6^{std} are generalized of CLEFIA. For $GFS_6^{imp}(No.1)$, one of the relations between inputs and outputs for each seven consecutive round is as follows:

$$\mathbf{x_{i-2}} = \mathbf{z_{i-5}} \oplus \mathbf{z_{i-9}} \oplus \mathbf{z_{i-16}} \oplus \mathbf{x_{i-20}} \tag{15}$$

And finally we have:

$$\begin{aligned} x_{i-2}^c + x_{i-5}^c + x_{i-9}^c + x_{i-16}^c + x_{i-20}^c &\geq (n+1)bb_{i-2} \\ bb_{i-2} \leq x_{i-5}^c + x_{i-9}^c + x_{i-16}^c &\leq 3nbb_{i-2} \end{aligned} \tag{16}$$

Therefore, for the seventh round to next for each seven consecutive rounds switching feature must be added.

In eight sub-blocks type II GFS that consists of standard and improved structure [13], four MDS matrices $\mathbf{M_1}$, $\mathbf{M_2}$, $\mathbf{M_3}$ and $\mathbf{M_4}$ are recommended to apply. Inequalities that are obtained for switching feature in GFS_8^{std} are generalized of prior structure, and for $GFS_8^{imp}(No.1)$, one of the relations between inputs and outputs for each nine consecutive round is as follows:

$$\begin{aligned} x_{i-3}^c + x_{i-7}^c + x_{i-13}^c + x_{i-20}^c + x_{i-30}^c + x_{i-35}^c &\geq (n+1)bb_{i-3} \\ bb_{i-3} \leq x_{i-7}^c + x_{i-13}^c + x_{i-20}^c + x_{i-30}^c &\leq 4nbb_{i-3} \end{aligned} \tag{17}$$

Table 4, shows the results for standard and improved generalized Feistel structures with $n = 4$, by considering switching properties. We point out that in l sub-blocks structures, in order to have more powerful structure $\frac{l}{2}$ different MDS matrices must be applied. However, this process negatively impacts the costs on generalized Feistel structures with larger sub-blocks. Fortunately, although using less matrices in structures with larger sub-blocks makes them a bit weaker, such these structures are still efficient, and instead lead to reduce the costs significantly. The obtained results for GFS_8^{imp} with 2 MDS matrices and GFS_{12}^{imp} with 3 MDS matrices, which are listed in Table 4, are enough to emphasis our claim.

5 Counting the Linear Active S-boxes

It is well known that, because of duality between differential and linear attack, the method of counting the linear active S-boxes is identical to differential active S-boxes in many regards. As shown in [4, 11], counting the linear active S-boxes could be calculated by using the simple transformation in Figure 7.

Table 4. Minimum number of differential active S-boxes of generalized Feistel structures imposed by switching properties with n=4

	2 MDS matrices			3 MDS matrices			4 MDS matrices		5 MDS matrices		6 MDS matrices	
round	Feistel	CLEFIA	GFS_8^{imp}	GFS_6^{std}	GFS_6^{imp}	GFS_{12}^{imp}	GFS_8^{std}	GFS_8^{imp}	GFS_{10}^{std}	GFS_{10}^{imp}	GFS_{12}^{std}	GFS_{12}^{imp}
1	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2	2	2	2	2
4	5	6	6	6	6	6	6	6	6	6	6	6
5	6	8	8	8	8	8	8	8	8	8	8	8
6	10	12	12	12	12	12	12	12	12	12	12	12
7	10	14	14	14	14	14	14	14	14	14	14	14
8	11	18	26	18	25	26	18	23	18	26	18	26
9	12	20	29	21	27	29	21	26	21	29	21	29
10	15	22	34	25	31	41	26	32	25	37	25	37
11	16	24	37	28	33	44	31	36	28	40	28	42
12	20	28	42	34	36	56	36	44	36	49	36	50
13	20	30	43	37	38	61	41	46	39	51	39	54
14	21	34	47	38	43	67	48	49	47	54	45	65
15	22	36	49	42	46	69	50	52	51	56	50	72
16	25	38	53	44	52	72	53	56	58	62	56	77
17	26	40	55	48	55	75	56	60	64	66	62	79
18	30	44	64	50	59	79	59	67	68	70	67	85
19	30	46	67	54	61	81	62	69	72	78	75	88
20	31	50	72	57	64	92	66	77	74	83	85	..
21	32	52	74	61	67	..	69	80	78	88	88	..
22	35	55	83	64	72	..	73	86	80	95	92	..
23	36	56	84	69	76	..	76	88	84	97	94	..
24	40	59	88	73	81	..	80	91	87	..	..	..

We emphasize that, in linear cryptanalysis, Feistel structures with SP-functions convert to Feistel structures with PS-functions, and x^c denotes the summation representation of vector $\mathbf{\Gamma.x}$.

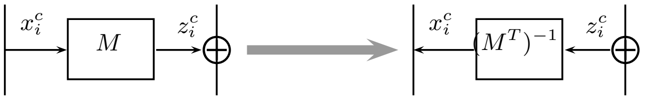

Fig. 7. transforming differential vectors to linear masks

Regardless of switching mechanism, if the matrix $\mathbf{M}$ be an MDS matrix, the number of linear active S-boxes for both standard and improved structures will be equal to differential active S-boxes. In case of using switching mechanism, in order to clarify, consider Figure 8 as a special example.

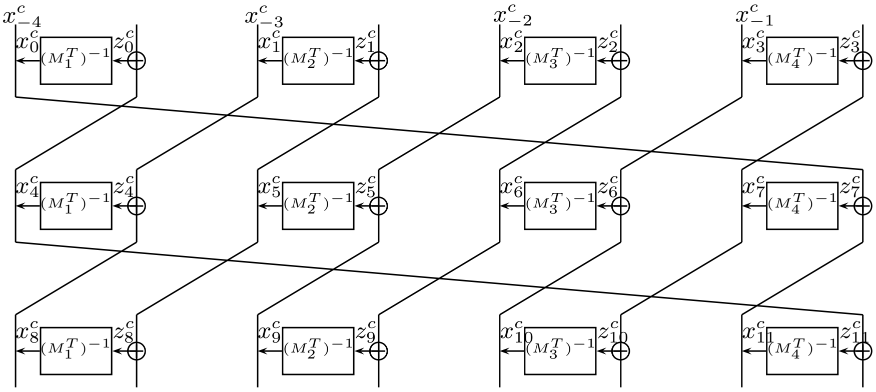

Fig. 8. Defining summation variables in GFS_8^{std} imposed by switching mechanism

The inequalities related to switching mechanism in linear cryptanalysis readily can be extracted from Theorem 3 in [11]. The relation (18) shows one of *4* relations between inputs and outputs of three consecutive round, in Figure 8:

$$\mathbf{\Gamma.x_5} = (\mathbf{M_2^T})^{\mathbf{-1}}\mathbf{\Gamma.x_1} \oplus (\mathbf{M_1^T})^{\mathbf{-1}}\mathbf{\Gamma.x_8} = \begin{bmatrix}(\mathbf{M_1^T})^{\mathbf{-1}} & (\mathbf{M_2^T})^{\mathbf{-1}}\end{bmatrix}\begin{bmatrix}\mathbf{\Gamma.x_1}\\ \mathbf{\Gamma.x_8}\end{bmatrix} \tag{18}$$

Without loss of generality, under the assumption that at least one of amounts $\mathbf{x_1}$ and $\mathbf{x_8}$ must be nonzero, by defining a new binary dummy variable bb_i, the relations (19) are obtained, based on the same process which was done for extracting the relations (12).

$$\begin{aligned} x_1^c + x_5^c + x_8^c &\geq (n+1)bb_i \\ bb_i \leq x_1^c + x_8^c &\leq 2nbb_i \end{aligned} \tag{19}$$

Due to obtained inequalities in (19), other inequalities can be obtained in a similar way. The results for standard and improved generalized Feistel structures with $n = 4$ by considering switching properties are listed in Table 5.

Table 5. Minimum number of linear active S-boxes of standard and improved generalized Feistel structures imposed by switching properties with n=4

round	Feistel	CLEFIA	GFS_6^{std}	GFS_6^{imp}	GFS_8^{std}	GFS_8^{imp}	GFS_{10}^{std}	GFS_{10}^{imp}	GFS_{12}^{std}	GFS_{12}^{imp}
1	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1
3	5	5	5	5	5	5	5	5	5	5
4	5	8	8	8	8	8	8	8	8	8
5	7	10	10	10	10	10	10	11	10	11
6	10	15	16	16	16	16	16	16	16	16
7	11	16	18	22	18	22	18	22	18	22
8	12	19	24	27	24	30	24	30	24	30
9	15	21	26	30	26	32	26	38	26	38
10	16	24	32	33	34	38	34	43	34	43
11	17	26	35	35	39	43	39	50	39	51
12	20	31	37	38	45	49	45	53	45	59
13	21	32	40	40	48	51	50	55	50	65
14	22	35	42	46	51	54	58	58	58	72
15	25	37	47	52	53	56	63	61	63	74
16	26	40	50	56	56	62	69	66	69	77
17	27	42	55	60	58	66	73	72	74	79
18	30	47	58	63	64	72	75	78	85	85
19	31	48	63	65	66	77	78	86	92	91
20	32	51	67	68	72	82	80	91	99	99
21	35	53	69	71	74	88	86	97	101	107
22	36	56	72	76	82	94	88	103	104	112
23	37	58	74	82	87	97	94	105	106	120
24	40	63	79	86	93	100	96	108	112	..

6 Conclusion

In this paper, by relying on MILP and summation representation, we introduced an efficient approach to calculate the number of differential and linear active S-boxes until *24* rounds. We first explained, how XOR relation and SP-function can be converted to inequalities. Then we listed the tables related to standard, and improved generalized Feistel structures. Moreover, we clarified the way of constructing inequalities related to employing multiple MDS matrices in generalized Feistel structures type II, and presented the results. Finally, we confirmed the effect of switching mechanism on linear cryptanalysis. Due to obtained results for linear cryptanalysis, it is clear that switching is more effective on linear cryptanalysis. Since, influence of switching on each GFS starts from third round to next, in linear cryptanalysis. Aside from the fact that our method does not apply for structures such as AES (because of $shiftrow$ operation), our approach significantly reduces the number of inequalities for other structures Compared with the previous approach based on MILP.

We would like to point out that, employing the multiple MDS matrices in improved *8* sub-blocks structures leads to enhance the number of active S-boxes almost 20 % for *18* rounds, and creates a structure so close to RIJNDAEL. Moreover, such a structure is appropriate to resist against quantum algorithms. For larger blocks, switching can not diffuse until *18* rounds, in differential cryptanalysis.

Besides that, in differential cryptanalysis, we have confirmed that in improved *8* sub-blocks structure, if we apply *2* different MDS matrices, only *3* differential active S-boxes is lower than applying *4* matrices after *24* rounds (*91* for *4* matrices and *88* for *2* matrices). By doing so, we not only benefit from switching features, but also apply fewer resources. It is worth mentioning that, our approach can be generalized for other Feistel structures, and is usable in designing future block ciphers.

References

1. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita. Camellia: A 128-bit Block Cipher Suitable for Multiple Platforms-Design and Analysis. In *SAC 2000*, volume 2012, pages 39–56. Springer-Verlag Berlin Heidelberg, 2001.
2. C. Beierle, J. Jean, S. Kolbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. Sim. The skinny family of block ciphers and its low-latency variant mantis, 2016.
3. A. Bogdanov. On unbalanced feistel networks with contracting MDS diffusion. *Designs, Codes and Cryptography*, 59(1):3558, 2011.
4. M. Kanda. Practical security evaluation against differential and linear cryptanalyses for feistel ciphers with spn round function. In *SAC 2000*, volume 2012, pages 324–338. Springer-Verlag, 2001.
5. N. Mouha, Gu Wang, Q., and B. D., Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *Inscrypt 2011*, volume 7537, pages 57–76. Springer-Verlag, 2012.
6. M. Sajadieh, A. Mirzaei, H. Mala, and V. Rijmen. A new counting method to bound the number of active s-boxes in Rijndael and 3d. *Designs, Codes and Cryptography*, 83(2):327–343, 2017.

7. K. Shibutani. On the diffusion of generalized feistel structures regarding differential and linear cryptanalysis. In *SAC 2010*, volume 6544, pages 211–228. Springer-Verlag, 2011.
8. T. Shirai and K. Araki. On generalized feistel structures using the diffusion switching mechanism. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E91-A(8):2120–2129, 2008.
9. T. Shirai, S. Kanamaru, and G. Abe. Improved upper bounds of differential and linear characteristic probability for camellia. In *FSE 2002*, volume 2365, pages 128–142. Springer-Verlag, 2002.
10. T. Shirai and K. Shibutani. Improving immunity of feistel ciphers against differential cryptanalysis by using multiple MDS matrices. In *FSE 2004*, volume 3017, pages 260–278. Springer-Verlag, 2004.
11. T. Shirai and K. Shibutani. On feistel structures using a diffusion switching mechanism. In *FSE 2006*, volume 4046, pages 41–56. Springer-Verlag, 2006.
12. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwataa. The 128-bit blockcipher clefia. In *FSE 2007*, volume 4593, pages 181–195. Springer-Verlag, 2007.
13. T. Suzaki and K. Minematsu1. Improving the generalized feistel. In *FSE 2010*, volume 6147, pages 19–39. Springer-Verlag, 2011.