Security Evaluation against Differential Cryptanalysis for Block Cipher Structures

Shengbao Wu[1,2], Mingsheng Wang[1]

1. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, PO Box 8718, China
2. Graduate School of Chinese Academy of Sciences, Beijing 100190, China
wushengbao@is.iscas.ac.cn
mingsheng_wang@yahoo.com.cn

Abstract. Estimating immunity against differential and linear cryptanalysis is essential in designing secure block ciphers. A practical measure to achieve it is to find the minimal number of active S-boxes, or a lower bound for this minimal number. In this paper, we provide a general algorithm using integer programming, which not only can estimate a good lower bound of the minimal differential active S-boxes for various block cipher structures, but also provides an efficient way to select new structures with good properties against differential cryptanalysis. Experimental results for the Feistel, CAST256, SMS4, CLEFIA and Generalized Feistel structures indicate that bounds obtained by our algorithm are the tightest except for a few rounds of the SMS4 structure. Then, for the first time, bounds of the differential active S-boxes number for the MISTY1, Skipjack, MARS and Four-cell structures are illustrated with the application of our algorithm. Finally, our algorithm is used to find four new structures with good properties against differential cryptanalysis. Security evaluation against liner cryptanalysis can be processed with our algorithm similarly by considering dual structures.

Key words: block cipher structures, active S-boxes, integer programming, differential cryptanalysis.

1 Introduction

An essential assignment of designing a block cipher is to ensure its security against known attacks, especially the two most important cryptanalysis approaches — differential cryptanalysis [2] and linear cryptanalysis [8]. A practical method to achieve it is to estimate the upper bounds of the maximum differential characteristic and linear trail probabilities.

In recent years, F-functions (See Fig.1) of many well-known block ciphers are designed with the same strategy named SP-type network that employs small nonlinear bijective functions (S-box) and a linear diffusion layer, such as Camellia [1], AES [5], CLEFIA [13] and SMS4 [6]. Since the only nonlinear part in a block cipher with SP-type F-function is S-box, evaluating the upper bounds of

the maximum differential characteristic (linear trail) probability is equivalent to counting the minimal number of differential (linear) active S-boxes in some consecutive rounds, or a lower bound for this minimal number.

There are two classes of methods to count the minimal number of differential (linear) active S-boxes for a block cipher structure with SP-type F-function. One shows it with proofs, which usually enumerate many possible cases artificially to obtain a lower bound. Proof results are useful to indicate the strength of block cipher structures, but sometimes valid for only restricted numbers of rounds. Kanda [7] got the first result for the security of Feistel structure, which then improved by Wang et.al [15]. Wu el.al [16] analyzed the CAST256 structure and obtained the lower bounds of active S-boxes for 8 and 16 round. The lower bounds of active S-boxes number for the CLEFIA and SMS4 structure were concerned by Shibutani [17] and Wang et.al [18] respectively.

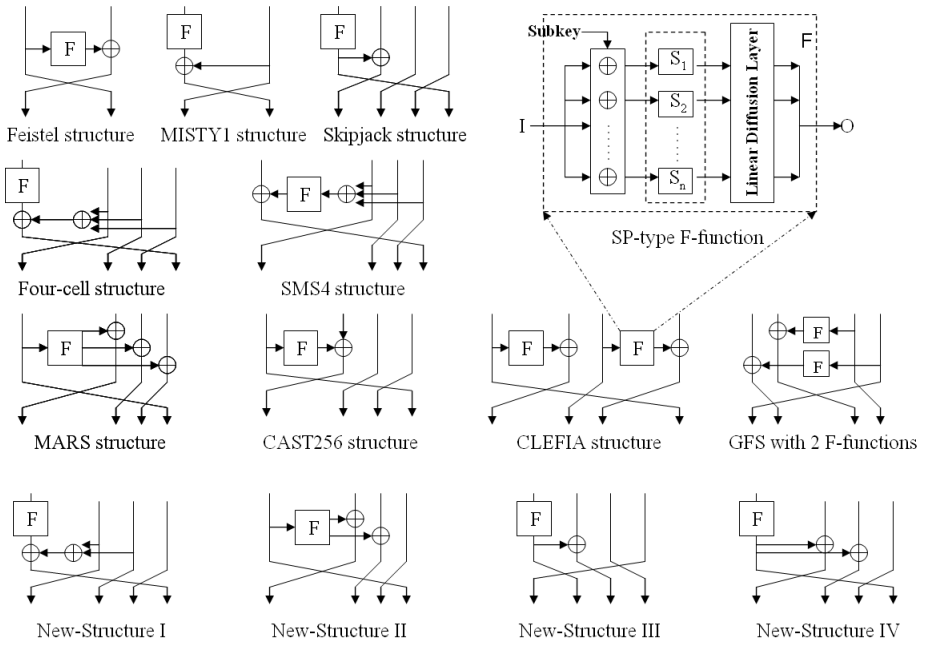

Fig. 1. Some well-known block cipher structures, SP-type F-function and several new structures with good properties against differential cryptanalysis.

Other approaches compute the number of active S-boxes with search algorithms. By modifying Matsui's algorithm in [9], Aoki et al. [1] showed an efficient algorithm to output lower bounds of the minimal number of active S-boxes for the Feistel structure. Shirai et al. [11, 12, 14] proposed some efficient search algorithms to estimate the security of the Feistel , CAST256, CLEFIA and general-

ized Feistel structures(GFS). A search algorithm is also proposed by Shibutani [17] to dispose the CLEFIA structure.

However, so far, known results are only limited in several structures. Security evaluation for many well-known structures with SP-type F-functions is unconscious, such as the MISTY, Skipjack, MARS and Four-cell structures. What's more, every known proof method or search algorithm is designed based on the specific observations of the target structure. There is not a general method to deal with many block cipher structures simultaneously.

In this work, we focus on counting the minimal number of differential active S-boxes for block cipher structures with SP-type F-functions. We provide a general algorithm using integer programming, which not only can estimate a good lower bound of the minimal differential active S-boxes for various block cipher structures, but also provides an efficient approach to find new structures with good properties against differential cryptanalysis. Because of the duality between differential characteristic and linear trail [3, 4], our algorithm can be easily extended to the linear cryptanalysis by considering its dual structure. Comparing with the best known results (theoretical or experimental results if they exist) for the Feistel, CAST256, SMS4, CLEFIA and Generalized Feistel structures, the lower bounds obtained by our algorithm are the tightest except for a few rounds of the SMS4 structure. Then, our algorithm is applied to the MISTY1, Skipjack, MARS and Four-cell structures. We get the lower bound of differential active S-boxes for these structures for the first time. Finally, our algorithm is used to find new structures with good properties against differential and linear cryptanalysis. We list four of them in Fig.1, which named as New-Structure I, II, III and IV respectively.

This paper is organized as follows. Section 2 introduces some preliminaries. The algorithm for computing the minimum number of active S-boxes is presented in Section 3. Experimental results of the well-known structures and the new structures are reported in Section 4. Finally, we conclude this paper in Section 5.

2 Preliminaries

2.1 Block Cipher Model

In this subsection, we describe structures in Fig.1 with a general model. The operation between data blocks and in the key addition layer is exclusive-OR.

Definition 1. *A (b, n_s, r) SP-type block cipher is a block cipher with b data branches, r rounds and n_s SP-type F-functions in a round, where all F-functions in this r-round block cipher are same.*

Let $x_{k,i}$ be the input data of i-th branch, $I_{k,j}, O_{k,j}$ be the input data and output data of the j-th F-function (from right to left) in round k respectively $(i = 1, 2, \ldots, b, j = 1, 2, \ldots, n_s)$. The k-th round relations of a (b, n_s, r) SP-type

block cipher can be represented generally as the following model:

$$\begin{aligned} I_{k,j} &= f_j(x_{k,1}, x_{k,2}, \ldots, x_{k,b}) = \bigoplus_{p=1}^{b} \alpha_{j,p} \cdot x_{k,p}, \quad (j = 1, 2, \ldots, n_s) \\ x_{k+1,i} &= g_i(x_{k,1}, x_{k,2}, \ldots, x_{k,b}, O_{k,1}, O_{k,2}, \ldots, O_{k,n_s}) \\ &= \bigoplus_{p=1}^{b} \zeta_{i,p} \cdot x_{k,p} \oplus \bigoplus_{q=1}^{n_s} \eta_{i,q} \cdot O_{k,q}, \quad (i = 1, 2, \ldots, b) \end{aligned}$$

where $\alpha_{j,p}, \beta_{j,q}, \zeta_{i,p}, \eta_{i,q} \in \{0, 1\}$. For the convenience of discussions, the notations $x_{k,i}$, $I_{k,j}$ and $O_{k,j}$ will be renamed as $x_{b\cdot(k-1)+i}$, $I_{n_s\cdot(k-1)+j}$ and $O_{n_s\cdot(k-1)+j}$ respectively in the subsequent discussions.

For example, the Feistel structure with SP-type F-function is a $(2, 1, r)$ SP-type block cipher. Its k-th round relations are:

$$I_k = x_{2\cdot(k-1)+2};\ x_{2\cdot k+1} = x_{2\cdot(k-1)+2};\ x_{2\cdot k+2} = x_{2\cdot(k-1)+1} \oplus O_k.$$

Moreover, the MISTY1, Skipjack, CAST256, SMS4, MARS, Four-cell, CLEFIA and GFS structures with SP-type F-function are in the block cipher model. Of course, many structures that don't list in Fig.1 are included in this model. Note that, equations in the block cipher model above are also hold when each data is substituted to its difference. Such equations are called *difference-based* relations of a block cipher structure.

2.2 Solve Linear Systems and Integer Programming

Gauss-Jordan elimination [20] can be adopted to solve a linear system, which gets the solution by reducing the augmented matrix of this system to reduced row echelon form using elementary row operations.

Sometimes, we must consider the optimization problem:

$$\min \quad \sum_{j=1}^{N} c_j x_j, \quad \text{subject to} \tag{1}$$

$$\begin{cases} \sum\limits_{j=1}^{N} a_{ij} x_j \geq d_i \quad (i = 1, 2, \ldots, M) \\ x_j \text{ integer} \quad (\text{for some or all } j = 1, 2, \ldots N) \end{cases} \tag{2}$$

This problem is called the (linear) integer programming problem [21]. It is named a *pure* integer programming when *all* decision variables must be integers.

Magma [19] is a mathematical software package suitable for solving linear systems and integer programming problems. What should be stressed here is that we must avoid integer programming problems with many variables and constraint conditions since integer programming is NP-hard.

2.3 Definitions

Let ΔI denotes the difference of I. Then, the following definitions are used in this paper.

Definition 2. *Let $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_2^{mn}$, where $\lambda_j \in \mathbb{F}_2^m$ $(1 \leq j \leq n)$. The hamming weight* wt *of λ is denoted as the number of nonzero components in λ, that is,* $\mathrm{wt}(\lambda) = \#\{\lambda_j \mid \lambda_j \neq 0, 1 \leq j \leq n\}$.

Definition 3. *Let a (b, n_s, r) SP-type block cipher be given. A differential input pattern is a vector $v \in \{0,1\}^{n_s \cdot r}$, where the i-th element of v is $'0'$ represents that $\Delta I_i = 0$, $'1'$ represents that $\Delta I_i \neq 0$.*

Definition 4. *The differential branch number of a linear diffusion layer P in the F-function is defined as $\mathcal{B}_d = \min_{\Delta\lambda \neq 0}\{\mathrm{wt}(\Delta\lambda) + \mathrm{wt}(P(\Delta\lambda))\}$, where $\Delta\lambda$ is the input difference of P.*

Since the key addition layer, S-boxes and linear diffusion layer P are bijective in an SP-type F-function, we have (1) $\Delta O = 0$ if and only if $\Delta I = 0$ and $\Delta O \neq 0$ if and only if $\Delta I \neq 0$; (2) $\mathcal{B}_d = \min_{\Delta I \neq 0}\{\mathrm{wt}(\Delta I) + \mathrm{wt}(\Delta O)\}$.

3 Algorithm

In this section, we present a united algorithm to compute a lower bound of the minimal number of differential active S-boxes for any r-round structure included in the (b, n_s, r) model.

3.1 Idea of the Algorithm

For a given (b, n_s, r) block cipher structure, all r round difference-based relations concerning with the structure can be viewed as a homogeneous linear system Φ_r with variables $(\Delta x_1, \Delta x_2, \ldots, \Delta x_{b\cdot(r+1)}, \Delta I_1, \ldots, \Delta I_{r\cdot n_s}, \Delta O_1, \ldots, \Delta O_{r\cdot n_s})$. Φ_r has at least one solution, known as the zero solution. But it's a trivial solution when we consider differential cryptanalysis.

To compute the minimal number of differential active S-boxes D_r, we need to solve linear system Φ_r and compute the number of active S-boxes involved in each nontrivial solution. But it's difficult to do this. For one thing, the specification of F-functions is unknown, which results in the impossibility of checking whether every solution is correct; For another, the computational ability might be another problem to obtain all concrete solutions.

To conquer these difficulties, we try to find a lower bound of D_r in our algorithm. Firstly, the limitation of F-functions is relaxed. For a given input difference $\Delta I \neq 0$, the output difference ΔO can be any nonzero difference. This relaxation may increase the solutions of Φ_r, which leads our algorithm to find only a lower bound of D_r. Then, linear system Φ_r is divided into $2^{n_s \cdot r}$ restricted linear systems Φ_r^v according to the $2^{n_s \cdot r}$ possible differential input patterns v of $(\Delta I_1, \ldots, \Delta I_{r\cdot n_s})$. For a given v, Φ_r^v is constructed by adding linear equations

$\Delta I_i = 0$ and $\Delta O_i = 0$ to Φ_r for all $v_i = 0$. Finally, for each restricted linear system Φ_r^v, we solve it and exhaust all nontrivial solutions to deduce a lower bound of D_r^v, where $D_r^v = \min\{\sum_{i=1}^{n_s \cdot r} wt(\Delta I_i) : \text{for all nontrivial solutions satisfying } \Phi_r^v\}$. The final lower bound of $D_r = \min\{\text{lower bound of } D_r^v : \text{ for each } v \text{ that makes } \Phi_r^v \text{ have nontrivial solutions}\}$.

However, two questions arise in the final step. (**Q1**) For a given differential input pattern v, is there a nontrivial solution satisfying Φ_r^v? (**Q2**) How to evaluate a tight lower bound of D_r^v when Φ_r^v has at least a nontrivial solution?

Let M_r^v be the coefficient matrix of Φ_r^v with column ordering $(\Delta x_1, \Delta x_2, \ldots, \Delta x_{b\cdot(r+1)}, \Delta I_1, \ldots, \Delta I_{r\cdot n_s}, \Delta O_1, \ldots, \Delta O_{r\cdot n_s})$. And let $\overline{M_r^v}$ be the reduced row echelon form of M_r^v (See Fig.2). Expressions corresponding to $\overline{M_r^v}$ can be partitioned into Part I and Part II. Part I consists of expressions involving ΔI_is, ΔO_is and at least one of Δx_is as variables; Part II consists of expressions only containing ΔI_is and ΔO_js as variables.

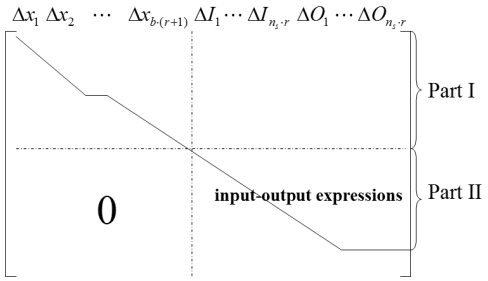

Fig. 2. A possible form of $\overline{M_r^v}$, where all nonzero elements lie above the echelon line.

Now, question **Q1** can be solved by observing $\overline{M_r^v}$. On the one hand, there is only a zero (trivial) solution if the rank of $\overline{M_r^v}$ is equal to the number of columns; On the other hand, there is not any solution when we observe a contradiction in $\overline{M_r^v}$, which happens in such a manner: an equation $\Delta I_i = 0$ or $\Delta O_i = 0$ is found in Part II of $\overline{M_r^v}$ but v_i is 1 in the differential input pattern v.

Then, we consider question **Q2** for each differential input pattern v that passes through question **Q1**. According to D_r^v, the only useful part in a nontrivial solution for counting the number of active S-boxes is the value of $(\Delta I_1, \ldots, \Delta I_{n_s \cdot r})$. And every solution satisfying Part II of $\overline{M_r^v}$ can be extended to at least a solution satisfying all expressions in $\overline{M_r^v}$ with same active S-boxes. So, we only concern solutions satisfying expressions in Part II of $\overline{M_r^v}$. Although we still can't exhaust all of them, some useful rules may help us to estimate the number of active S-boxes $wt(\Delta I_i)$. For example, $\mathrm{wt}(\Delta I_i) = 0$ if $\Delta I_i = 0$, and $\mathrm{wt}(\Delta I_i) \geq 1$, $\mathrm{wt}(\Delta I_i) + \mathrm{wt}(\Delta O_i) \geq \mathcal{B}_d$ if $\Delta I_i \neq 0$. For a further step, we have some more observations:

Proposition 1. *Let an input-output expression be given:*

$$\Delta I_{u_1} \oplus \Delta I_{u_2} \oplus \cdots \oplus \Delta I_{u_p} = \Delta O_{w_1} \oplus \Delta O_{w_2} \oplus \cdots \oplus \Delta O_{w_q}$$

where $u_i, w_j \in \{1, 2, \ldots, n_s \cdot r\}$, $p + q \geq 2$, *and* $\Delta I_{u_i} \neq 0, \Delta O_{w_j} \neq 0$ *for all* $i = 1, \ldots, p$, $j = 1, \ldots, q$. *Then we have*

1) If $(p = 1$ *or* $q = 1)$ *and* $u_i \neq w_j$ *for all* $i = 1, \ldots, p$ *and* $j = 1, \ldots, q$, *then*

$$\sum_{i=1}^{p} \mathrm{wt}(\Delta I_{u_i}) + \sum_{j=1}^{q} \mathrm{wt}(\Delta I_{w_j}) \geq \mathcal{B}_d, \tag{3}$$

2) If $p = 1$ *and there exists a* $j_0 \in \{1, 2, \ldots, q\}$ *subjecting to* $u_1 = w_{j_0}$, *then*

$$2\mathrm{wt}(\Delta I_{u_1}) + \sum_{j \in \{1,\ldots,q\} \setminus \{j_0\}} \mathrm{wt}(\Delta I_{w_j}) \geq \mathcal{B}_d, \tag{4}$$

3) If $q = 1$ *and there exists an* $i_0 \in \{1, \ldots, p\}$ *subjecting to* $u_{i_0} = w_1$, *then*

$$2\mathrm{wt}(\Delta I_{w_1}) + \sum_{i \in \{1,\ldots,p\} \setminus \{i_0\}} \mathrm{wt}(\Delta I_{u_i}) \geq \mathcal{B}_d, \tag{5}$$

4) If $(p = 2$ *and* $q = 0)$ *or* $(p = 0$ *and* $q = 2)$, *then*

$$\mathrm{wt}(\Delta I_{u_1}) = \mathrm{wt}(\Delta I_{u_2}) \qquad or \qquad \mathrm{wt}(\Delta I_{w_1}) = \mathrm{wt}(\Delta I_{w_2}), \tag{6}$$

5) Else, $\mathrm{wt}(\Delta I_{u_i}) \geq 1, \mathrm{wt}(\Delta I_{w_j}) \geq 1, i = 1, \ldots, p, j = 1, \ldots, q$.

Proof. Clearly, $\mathrm{wt}(\Delta I_i) = \mathrm{wt}(\Delta P^{-1}(O_i))$.

1) If $q = 1$, then $\sum\limits_{i=1}^{p} \mathrm{wt}(\Delta I_{u_i}) + \mathrm{wt}(\Delta I_{w_1}) \geq \mathrm{wt}(\bigoplus\limits_{i=1}^{p} \Delta I_{u_i}) + \mathrm{wt}(\Delta I_{w_1}) = \mathrm{wt}(\Delta O_{w_1}) + \mathrm{wt}(\Delta I_{w_1}) \geq \mathcal{B}_d$.
If $p = 1$, then $\Delta I_{u_1} = \bigoplus\limits_{j=1}^{q} \Delta O_{w_j} = P(\bigoplus\limits_{j=1}^{q} \Delta P^{-1}(O_{w_j})) = P(\Delta \bigoplus\limits_{j=1}^{q} P^{-1}(O_{w_j}))$.
Hence $\mathrm{wt}(\Delta I_{u_1}) + \sum\limits_{j=1}^{q} \mathrm{wt}(\Delta I_{w_j}) = \mathrm{wt}(\Delta I_{u_1}) + \sum\limits_{j=1}^{q} \mathrm{wt}(\Delta P^{-1}(O_{w_j}))$
$\geq \mathrm{wt}(P(\Delta \bigoplus\limits_{j=1}^{q} P^{-1}(O_{w_j}))) + \mathrm{wt}(\Delta \bigoplus\limits_{j=1}^{q} P^{-1}(O_{w_j})) \geq \mathcal{B}_d$.
2) Without loss of generality, let $j_0 = 1$. Using the same reasons as in 1), we have $2\mathrm{wt}(\Delta I_{u_1}) + \sum\limits_{j=2}^{q} \mathrm{wt}(\Delta I_{w_j}) = \mathrm{wt}(\Delta I_{u_1}) + \sum\limits_{j=1}^{q} \mathrm{wt}(\Delta P^{-1}(O_{w_j})) \geq \mathcal{B}_d$.
3) Without loss of generality, let $i_0 = 1$. Then, $2\mathrm{wt}(\Delta I_{w_1}) + \sum\limits_{i=2}^{p} \mathrm{wt}(\Delta I_{u_i}) \geq \mathrm{wt}(\bigoplus\limits_{i=1}^{p} \Delta I_{u_i}) + \mathrm{wt}(\Delta I_{w_1}) = \mathrm{wt}(\Delta O_{w_1}) + \mathrm{wt}(\Delta I_{w_1}) \geq \mathcal{B}_d$.

4) Obviously, when $p = 2$ and $q = 0$, we have $\mathrm{wt}(\Delta I_{u_1}) = \mathrm{wt}(\Delta I_{u_2})$. If $p = 0$ and $q = 2$, then $\Delta O_{w_1} = \Delta O_{w_2}$. Hence $\Delta P^{-1}(O_{w_1}) = \Delta P^{-1}(O_{w_2})$. So, $\mathrm{wt}(\Delta I_{w_1}) = \mathrm{wt}(\Delta P^{-1}(O_{w_1})) = \mathrm{wt}(\Delta P^{-1}(O_{w_2})) = \mathrm{wt}(\Delta I_{w_2})$.
5) In this case, no obvious relations between ΔI_{u_i} $(i = 1, \ldots, p)$ or ΔO_{w_j} $(j = 1, \ldots, q)$ can be found. So, we only know that $\mathrm{wt}(\Delta I_{u_i}) \geq 1$, and $\mathrm{wt}(\Delta I_{w_j}) \geq 1$ for $i = 1, \ldots, p, j = 1, \ldots, q$.

Let Λ_r^v be the expressions in Part II of $\overline{M_r^v}$ except all $\Delta I_i = 0$ and $\Delta O_i = 0$, S_r^v be the linear space generated by the expressions in Λ_r^v over $\mathbb{F}_2$. [1] Then, all input-output expressions which fulfill the requirements in proposition 1 are contained in $S_r^v \backslash \{0\}$. Now, the second question **Q2** for a given differential input pattern v is reduced to solve the following pure integer programming problem:

$$\min \quad \sum_{i=1}^{r \cdot n_s} \mathrm{wt}(\Delta I_i), \text{ subject to} \tag{7}$$

$$\begin{cases} \text{Inequalities and equations deduced from } S_r^v \backslash \{0\} \text{ by proposition 1} \\ \mathrm{wt}(\Delta I_i) = 0 \text{ if } v_i = 0 \\ \mathrm{wt}(\Delta I_i) \geq 1 \text{ if } v_i = 1 \end{cases} \tag{8}$$

3.2 An Algorithm

By the analysis of subsection above, the pseudo-code of a basic algorithm for estimating a lower bound of D_r is described as follows.

Input: The k-th round difference-based relations of a given structure.
Output: A lower bound of D_r.

$D_r \leftarrow \infty$;
Generate the linear system Φ_r;
for *every differential input pattern* v **do**
  Generate the restricted linear system Φ_r^v and adopt *Gauss-Jordan elimination* to obtain the reduced row echelon form matrix $\overline{M_r^v}$;
  if v *is a pattern which passes through the question* **Q1 then**
    Obtain the linear space S_r^v;
    if $S_r^v \backslash \{0\} = \emptyset$ **then**
      $D_r^v = wt(v)$;
    else
      Use proposition 1 to select all useful constraint conditions supplied by expressions in $S_r^v \backslash \{0\}$ and solve the integer programming problem (7) to obtain a lower bound D_r^v;
    If $D_r^v < D_r$, then $D_r \leftarrow D_r^v$;
return D_r.

Algorithm 1: Pseudo-code of a basic algorithm for computing D_r

[1] S_r^v is denoted as $\{0\}$ if Λ_r^v is an empty set.

Algorithm Complexity. The time complexity of this algorithm is dominated by step **1**, **7** and **8** in **Algorithm** 1. However, it's hard to achieve the accurate time complexity because the elimination of differential input patterns in step **3** and the number of constraint conditions obtained in step **7** vary from structure to structure. The worst size of constraint conditions for a given r-round block cipher structure is $2^{r\cdot n_s}-1$. So, the worst case of this algorithm should solve $2^{r\cdot n_s}$ integer programming problems with $r\cdot n_s$ variables and $2^{r\cdot n_s}-1$ constraint conditions.

3.3 An Improved Algorithm

In general, **Algorithm** 1 may be inefficient because S_r^v contains all linear relations derived from Λ_r^v. In this subsection, we present an improved algorithm. We try to improve the dominating steps **1**, **7** and **8** of **Algorithm** 1 in two aspects. For one thing, using the results of smaller rounds to reduce the times of solving integer programming problems. This idea is proposed by Matsui [9] and used in [14]; For another, reducing the number of input-output expressions involved in step **4** can reduce the size of integer programming problems. That is, we only consider a subset $S_{r,e}^v \subseteq S_r^v\backslash\{0\}$ in the improved algorithm.

How to choose a suitable subset $S_{r,e}^v$ of input-output expressions is a challenging problem. On the one hand, a large $S_{r,e}^v$ may generate many reduplicate constraint conditions that affect the efficiency of the algorithm; On the other hand, a small $S_{r,e}^v$ may miss some useful constraint conditions that influence the tightness of results.

By comparing many experimental results, we suggest a manner here. Let $M_{r,e}^v$ be the coefficient matrix of Φ_r^v with column ordering $(\Delta x_1, \Delta x_2, \ldots, \Delta x_{b\cdot(r+1)}, \Delta O_1, \ldots, \Delta O_{r\cdot n_s}, \Delta I_1, \ldots, \Delta I_{r\cdot n_s})$. That is, in the matrix M_r^v, we exchange its $(b\cdot(r+1)+j)$-th column with $(b\cdot(r+1)+r\cdot n_s+j)$-th column for all $j=1,\ldots,r\cdot n_s$. Similarly, we have a corresponding matrix $\overline{M_{r,e}^v}$ and an expression set $\Lambda_{r,e}^v$ here. Now $S_{r,e}^v$ consists of four parts: i) Expressions in Λ_r^v; ii) Expressions in $\Lambda_{r,e}^v$; iii) The sum of every two distinct expressions in Λ_r^v over $\mathbb{F}_2$; iv) The sum of every two distinct expressions in $\Lambda_{r,e}^v$ over $\mathbb{F}_2$.

Instead of considering all 2^l-1 input-output expressions in $S_r^v\backslash\{0\}$, the size of $S_{r,e}^v$ is reduced to $l\cdot(l+1)$ now, where l is the number of expressions in Λ_r^v.

In the improved algorithm **Algorithm** 2, we use D_i to store the minimal number of active S-boxes for i-round block cipher. **Set** is used to store the information of foregoing rounds. Every element E in **Set** has four components: $E[1]$ is a differential input pattern which belongs to $\{0,1\}^{n_s\cdot(i-1)}$, where i is the number of current round; $E[2]$ represent the round number of $E[1]$, that is, $E[2]=i-1$; $E[3]$ is a lower bound of $D_{i-1}^{E[1]}$; $E[4]$ indicates the corresponding round number of $E[3]$. Binary(j,n_s) converts the integer j into a binary vector with length n_s. $a||b$ combines vector a and b to a new vector. For example, $[0,1]||Binary(1,2)=[0,1]||[0,1]=[0,1,0,1]$.

Remark 1. In step **1** of **Algorithm** 2, $E[3]+D_{E[2]-E[4]}\geq D_{E[2]}$ means that the lower bound of this differential input pattern is not less than current $D_{E[2]}$. So,

the value of $D_{E[2]}$ will not be renewed in this case, which means that we don't need to solve the integer programming problem here.

Input: The k-th round difference-based relations of a given structure.
Output: Lower bounds of D_i for $0 \le i \le r$.

$D_0 \leftarrow 0$, $D_i \leftarrow \infty (i = 1 \dots r)$ and **Set** $\leftarrow \{[[], 0, 0, 0]\}$;
for $i \leftarrow 1$ *to* r **do**
  Generate the linear system Φ_i;
  $[\mathbf{Set}, D_i] = \mathbf{SubFun(Set,}\Phi_i\mathbf{)}$;
return $D_i (i = 1, \dots, r)$;

SubFun(Set,Φ_i)
 tempSet $\leftarrow \emptyset$;
while Set $\neq \emptyset$ **do**
  $E \leftarrow Random(\mathbf{Set})$; `/* Select a random element in Set. */`
  for $j \leftarrow 0$ *to* $2^{n_s} - 1$ **do**
    $v \leftarrow E[1] || \text{Binary}(j, n_s)$, $E[2] \leftarrow E[2] + 1$;
    Obtain the restricted linear system $\Phi^v_{E[2]}$ and adopt *Gauss-Jordan elimination* to obtain the matrix $\overline{M^v_{E[2]}}$;
    if *v is a pattern which passes through the question* **Q1 then**
1   **if** $E[3] + D_{E[2]-E[4]} < D_{E[2]}$ **then**
        Compute $D^v_{E[2]}$ by using the step **4** to **8** of **Algorithm** 1. Of course, $S^v_{E[2]} \backslash \{0\}$ is replaced by $S^v_{E[2],e}$ here;
        tempSet $\leftarrow$ tempSet $\cup \{[v, E[2], D^v_{E[2]}, E[2]]\}$;
        If $D^v_{E[2]} < D_{E[2]}$, then $D_{E[2]} \leftarrow D^v_{E[2]}$;
      else
        tempSet $\leftarrow$ tempSet $\cup \{[v, E[2], E[3], E[4]]\}$;
  Set $\leftarrow$ **Set** $\setminus \{E\}$;
Set $\leftarrow$ tempSet;
return $[\mathbf{Set}, D_i]$;

Algorithm 2: Pseudo-code of an improved algorithm for computing D_r

Algorithm Complexity. The worst time complexity of this algorithm for the final round should solve $2^{r \cdot n_s}$ integer programming problems with $r \cdot n_s$ variables and $O(r^2 \cdot n_s^2)$ constraint conditions. And it costs $4 \cdot (r-1) \cdot n_s \cdot 2^{(r-1) \cdot n_s}$ bits at most to store the temporary **Set**, where 4 is the number of components in every element E and $(r-1) \cdot n_s$ is the binary length of $E[1]$ which is the dominating component in E for storage.

4 Experimental Results

In this section, we compute lower bounds of D_r for various block cipher structures (See Fig.1) with SP-type F-function by running **Algorithm 2** on Magma. We

directly use the function "MinimalIntegerSolution" provided in Magma to solve integer programming problems. The function returns a vector which represents an optimal solution of the problem. What we are interested is the minimal sum of the optimal solutions for some consecutive rounds of a structure.

We choose $\mathcal{B}_d = 5$ to illustrate experimental results since it is a widely used branch number in many well-known block ciphers, such as AES, Camellia, CLEFIA and SMS4. And all results for a structure list in Table 1 can be got in hours on a 2.66 Ghz processor. We record results up to 25 or 26 F-functions ($\lceil \frac{25}{n_s} \rceil$ rounds) for all structures illustrated in Fig.1 except for the SMS4 and MARS structures, whose results are only up to 21 rounds.

Table 1. Lower bounds of D_r for some block cipher structures

	Comparison Results										First Results				New Structures			
	fei		cas		cle		gfs		sms		mis	ski	mar	fou	I	II	III	IV
r	[15]	itp	[14]	itp	[14]	itp	[14]	itp	[18]	itp	itp	itp	itp	itp	itp	itp	itp	itp
1	0	0	0	0	0	0	0	0	-	0	0	0	0	0	0	0	0	0
2	1	1	0	0	1	1	0	0	-	0	1	0	0	0	0	0	0	0
3	2	2	0	0	2	2	1	1	-	0	2	0	0	0	0	0	0	0
4	5	5	1	1	6	6	2	2	-	1	5	1	1	1	1	1	1	1
5	6	6	1	1	8	8	5	5	-	2	6	1	2	2	1	1	1	1
6	7	7	1	1	12	12	6	6	-	2	7	1	2	2	2	2	1	2
7	8	8	2	2	12	12	7	7	5	5	10	2	5	2	3	6	4	3
8	11	11	6	6	13	13	8	8	6	6	11	6	6	5	6	6	6	6
9	12	12	6	6	14	14	9	9	7	7	12	6	7	6	6	6	6	6
10	13	13	7	7	18	18	10	10	8	8	14	7	8	9	6	8	7	8
11	14	14	7	7	20	20	11	11	$\underline{9}$	8	16	7	8	10	7	9	8	9
12	17	17	8	8	24	24	12	12	10	10	17	8	10	10	9	11	9	11
13	18	18	9	9	24	24	13	13	$\underline{11}$	10	19	9	10	10	10	12	10	11
14	19	19	13	13	-	-	-	-	$\underline{11}$	10	21	13	10	11	10	13	13	12
15	20	20	14	14	-	-	-	-	12	12	22	13	12	12	13	14	14	15
16	23	23	16	16	-	-	-	-	13	13	24	16	13	12	15	15	17	15
17	24	24	17	17	-	-	-	-	14	15	26	17	15	12	15	16	18	15
18	25	25	17	17	-	-	-	-	15	15	27	17	15	15	15	18	19	16
19	26	26	18	18	-	-	-	-	16	16	29	18	16	16	16	18	21	17
20	29	29	18	18	-	-	-	-	16	18	31	20	18	19	17	20	21	17
21	30	30	19	19	-	-	-	-	17	18	32	20	18	20	18	21	23	18
22	31	31	19	19	-	-	-	-	18	-	34	21	-	20	20	22	24	21
23	32	32	20	20	-	-	-	-	19	-	36	22	-	20	21	22	25	21
24	35	35	24	24	-	-	-	-	20	-	37	25	-	21	21	24	26	23
25	36	36	24	24	-	-	-	-	21	-	39	26	-	22	22	25	27	24

* We use the first three ordinary letters of a structure's name to indicate it.
* 'itp' means the results obtained by our algorithms in this paper.

4.1 Compare with Known Results

Results obtained by our algorithms in this paper for the Feistel, CAST256, CLEFIA, GFS with 2 F-functions and SMS4 structures are shown in the first big column of Table 1. For comparison, the best previous results (theoretical or experimental results if they exist) are also illustrated. From the result table 1, we observe that lower bounds of D_r obtained by our algorithms are the tightest except for only a few rounds of the SMS4 structures, which are round 11,13 and 14. Comparison results demonstrate that our algorithms is correct and acquire tight bounds.

4.2 Apply to Other Well-known Structures

With the application of our algorithm, we give the first security evaluation for the MISTY, Skipjack, MARS and Four-cell structures against differential cryptanalysis in the second big column of Table 1.

In [10], the conclusion shows that the MISTY1 structure is structurally stronger than the Feistel structure with both differential and linear cryptanalysis under the condition that all S-boxes are bijective. The result of our algorithm confirms this again when they have the same SP-type F-function.

For $r \leq 21$ rounds, we observe that the lower bounds of D_r for the MARS structure are same to that of the SMS4 structure when they have same $\mathcal{B}_d$. In fact, it's the dual structure of the SMS4 structure, which indicates that the SMS4 structure has same immunity against differential and linear cryptanalysis.

4.3 Find New Structures

Although many structures have been adopted in designing block ciphers, the number of them is negligible in comparison with that included in the general (b, n_s, r) model. Some structures with good immunity against differential and linear cryptanalysis may hide in this model. Our algorithms provide a way to select them out. In Fig.1, we display four of them, which are named as New-Structure I, II, III and IV respectively.

SMS4 is a concrete 128-bit block cipher in the $(4, 1, r)$ SP-type block cipher model with $\mathcal{B}_d = 5$. Since the maximum differential probability p_s for an active S-box in SMS4 is $p_s = 2^{-6}$, we need at least 22 active S-boxes to guarantee its immunity against differential cryptanalysis. Look up lower bounds in Table 1 and [18], 26 round [2] of SMS4 is requested to provide 22 active S-boxes.

If we replace the underlying structure of SMS4 with other structures in the $(4, 1, r)$ block cipher model in Fig.1, we conclude that other structures require less rounds (See Table 2) for immunity against differential cryptanalysis than the SMS4 structure except the MARS structure.

Results in Table 2 indicate that we indeed find some new structures with good properties against differential cryptanalysis. Especially for the New-Structure II

[2] Although we don't get this bound by our algorithm directly, we can harness the lower bounds of 9 round and 17 round to achieve it.

Table 2. Rounds needed for providing 22 active S-boxes

Name	SMS4	MARS	CAST256	Skipjack	Four-cell	New I	New II	New III	New IV
Round	26	26	24	23	25	25	22	21	24

and III, they are better than any other well-known structures involved in Table 2.

5 Conclusions

In this paper, a unified algorithm is proposed to evaluate the lower bounds of the minimal number of differential active S-boxes for block cipher structures contained in the general model, which includes the Feistel, MISTY1, CAST256, Skipjack, SMS4, CLEFIA, MARS, Four-cell and GFS structures as instances. Although it's a general algorithm, our experimental results have indicated its exactness and efficiency.

Thanks to the symmetrical role of ΔI_{u_i} and ΔO_{w_j} in Proposition 1, our algorithm can be directly used in linear cryptanalysis to count the minimal number of linear active S-boxes by considering the dual structures.

Moreover, our algorithms provide an approach to find new structures with good properties against differential cryptanalysis in the block cipher model of section 2. Some new structures are displayed in Fig.1. We believe that more useful structures can be found with the help of our algorithm.

References

1. Aoki, K., Ichikawa, T., Kanda, M., et al: Camellia: A 128-bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. Stinson, D. R., Tavares, S. (eds.) SAC 2000, LNCS, vol. 2012, pp. 39-56. Springer, Heidelberg (2001)
2. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, Vol.4, No.1, pp. 3-72 (1991)
3. Biham, E.: On Matsui's Linear Cryptanalysis. Santis, A. D. (eds.) Eurocrypt'94, LNCS, vol. 950, pp. 222-238. Springer, Heidelberg (1995)
4. Matsui, M.: On Correlation Between the Order of S-boxes and the Strength of DES. Santis, A. D. (eds.) Eurocrypt'94, LNCS, vol. 950, pp. 366-375. Springer, Heidelberg (1995)
5. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag (2002)
6. Diffe, W, Ledin, G(translators).: SMS4 Encryption Algorithm for Wireless Networks. Cryptology ePrint Archive, report 2008/329, received 29 Jul 2008. `http://eprint.iacr.org/`
7. Kanda, M.: Practical Security Evaluation against Differential and Linear Cryptanalyses for Feistel Ciphers with SPN round function. Stinson, D. R., Tavares, S. (eds.) SAC'2000, LNCS, vol. 2012, pp. 324-338. Springer, Heidelberg (2001)
8. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. Helleseth, T. (eds.) EUROCRYPT'93, LNCS, vol. 765, pp. 386-397. Springer, Heidelberg (1994)

9. Matsui, M.: Differential Path Search of the Block Cipher E2. Technical Report, ISEC99-19 (1999)
10. Matsui, M.: New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis. Gollmann, D. (eds.) FSE'96, LNCS, vol. 1039, pp. 205-217. Springer, Heidelberg (1996)
11. Shirai, T., Preneel, B.: On Feistel Ciphers Using Optimal Diffusion Mappings across Multiple Rounds. Lee, P. J. (eds.) Asiacrypt'04, LNCS, vol. 3329, pp. 1-15. Springer, Heidelberg (2004)
12. Shirai, T., Shibutani, K.: On Feistel Structures Using a Diffusion Switching Mechanism. Robshaw, M. (eds.) FSE'06, LNCS, vol. 4047, pp. 41-56. Springer, Heidelberg (2006)
13. Shirai, T., Shibutani, K., Akishita, T., et al.: The 128-bit Blockcipher CLEFIA. Biryukov, A. (eds.) FSE'07, LNCS, vol. 4593, pp. 181-195. Springer, Heidelberg (2007)
14. Shirai, T., Araki, K.: On Generalized Feistel Structures Using the Diffusion Switching Mechanism. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. vol. E91-A, No. 8, pp. 2120-2129 (2008)
15. Wang, N., Jin, C.: Security Evaluation against Differential and Linear Cryptanalyses for Feistel Ciphers. Frontiers of Computer Science in China, Vol.3(4) (2009)
16. Wu, W., Zhang, W., Lin, D.: On the Security of Generalized Feistel Scheme with SP Round Function. International Journal of Network Security, Vol.3, No.3, pp. 215-224 (2006)
17. Shibutani, K.: On the Diffusion of Generalized Feistel Structures Regarding Differential and Linear Cryptanalysis. Biryukov, A. (eds.) SAC 2010,LNCS, vol. 6544, pp. 211-228. Springer, Heidelberg (2011)
18. Wang, M., Liu, J., Wang, X.: The upper bounds on differential characteristics in block cipher SMS4. Cryptology ePrint Archive, report 2010/155, received 25 Mar 2010, `http://eprint.iacr.org/`
19. Bosma, W., Cannon, J., Playoust, C.: The MAGMA Algebra System I: The User Language. In Journal of Symbolic Computation, Vol. 24, Issues 3-4, pp. 235-265 (1997)
20. Meyer, C. D.: Matrix Analysis and Applied Linear Algebraic. Cambridge University Press (2001).
21. Nemhauser, G.L., Wolsey, L. A.: Integer and Combinatorial Optimization. John Wiley & Sons, Inc., New York (1998)