Jrl Syst Sci & Complexity (2010) : 1–??

Analysis of Minimum Numbers of Linearly Active S-Boxes of a Class of Generalized Feistel Block Ciphers

Xiaopei Guo · Kejian Xu · Tongsen Sun · Xiubin Fan

Received: / Revised:

Abstract For a class of generalized Feistel block ciphers, an explicit recurrent formula for the minimum numbers of linearly active S-boxes of any round r is presented.

Key words block cipher, generalized Feistel structure, linear spread value, the minimum number of linearly active S-boxes

1 Introduction

Linear cryptanalysis and differential cryptanalysis, the two most significant analyses methods applicable to block ciphers, were introduced by Matsui [1] and Biham, Shamir [2], respectively. Whether a block cipher can resist the two analyses is one of basic problems of the security of block ciphers. However, in the design of block ciphers, such ability is usually measured by minimum numbers of linearly or differentially active S-boxes. For AES, the branching number method is used to determine lower bounds for minimum numbers of linearly or differentially active S-boxes.

The formal definition of generalized *Feistel* Structure(GFS) was given by Zheng et al.[3]. Several cryptographic properties of these structures were analyzed in [4][5]. In 1992, Nyberg and Knudsen [6] first proposed the conception of a provable security against differential cryptanalysis and gave a provable security for a Feistel structure. In [7], Lee et al. discussed the provable security of the standard Type-II GFS with the partitioning number d against differential and linear attacks, and then Shirai and Araki discussed its practical security against differential and linear attacks in [8]. They showed the lower bounds on the numbers of active S-boxes for three types of generalized Feistel Structure: Type-I, Type-II and Nyberg's constructions [3][9]. Kanda [10] presented the minimum number of active S-boxs of Feistel ciphers with SPN round function. Using the minimum number of active S-boxes, Nyberg and Knudsen [11] gave the upper bounds of the maximum linear spread value and maximum differential spread value of Feistel system. Recently, Suzaki and Minematsu introduced a GFS with the optimal round permutation with respect to full diffusion property, which is a property that all

Xiaopei Guo
College of mathematics, Qingdao University, Qingdao 266071, *China*. E-mail: qdguoxiaopei@163.com.
Kejian Xu
College of mathematics, Qingdao University, Qingdao 266071, *China*. E-mail: kejianxu@amss.ac.cn.
Tongsen Sun
College of mathematics, Qingdao University, Qingdao 266071, *China*. E-mail: stscn2005@163.com.
Xiubin Fan
Institute of Software, Chinese Academy of Sciences, Beijing 100049, *China*. E-mail: fanxiubin1966@sina.com
This work was supported by the National Natural Science Foundation of China (Grant No. 10871106).

outputs are affected by all inputs [12]. Their paper showed that the improved GFS can be more secure against impossible differential and saturation attacks than the standard GFS. However, they expect that the minimum numbers of active S-boxes remains about the same. Thus their structures still require at least same number of rounds as the standard GFS to be secure against differential and linear attacks.

In the references [13] and [14], the authors discussed the linear cryptanalysis and differential cryptanalysis of the generalized Feistel ciphers respectively, and they gave the maximum linear spread value and differential spread value for 5–32 rounds through enumeration. Precisely, the structure discussed in [13] is as follows: The block length is 128 bits, the confusion part for the round function F is S-boxes with 8 bits input and 8 bits output, and the invertible transformation P for the diffusion part is:

$$P(X) = X \oplus (X <<< 6) \oplus (X <<< 14)$$
$$\oplus (X <<< 22) \oplus (X <<< 24),$$

where $X \in \mathbf{F}^{32}$ and $<<<$ denotes the left cyclic shift. Graphically, this can be presented as:

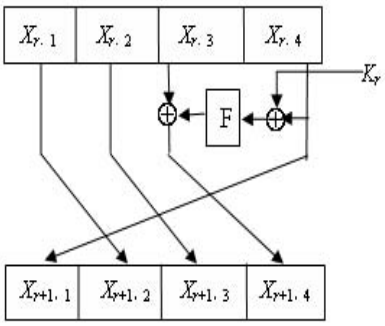

Figure 1: Feistel Structure

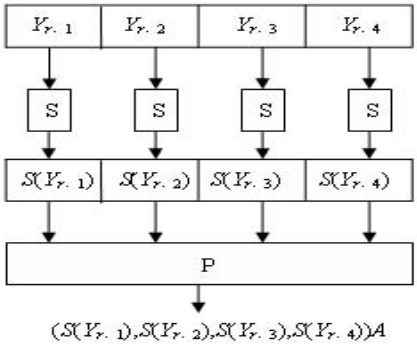

Figure 2: Round Function

The Feistel structure can be mathematically described as:

$$X_{r+1} := (X_{r+1,1}, X_{r+1,2}, X_{r+1,3}, X_{r+1,4})$$
$$:= (X_{r,4}, X_{r,1}, X_{r,2}, X_{r,3} \oplus F(X_{r,4} \oplus K_r)), \quad (1)$$

where $X_{t,l}, K_t \in \mathbf{F}^{32}, t \geq 0$, $l = 1, 2, 3, 4$, and if $Y_r := (Y_{r,1}, Y_{r,2}, Y_{r,3}, Y_{r,4})$, then

$$F(Y_r) = (S(Y_{r,1}), S(Y_{r,2}), S(Y_{r,3}), S(Y_{r,4}))A, \quad (2)$$

where $Y_r \in \mathbf{F}^{32}; Y_{r,i} \in \mathbf{F}^8, i = 1, 2, 3, 4$, and A is the invertible matrix corresponding to the invertible linear transformation P. Clearly, (2) is a layer of SP structure, and (1) moving one time is called one round. Assume that $X_{0,1}, X_{0,2}, X_{0,3}, X_{0,4}, K_t \in \mathbf{F}^{32}, t = 0, 1, 2, \ldots, N-1$, are independent and identically distributed random variables. Then, in [13], through enumeration the authors give the minimum numbers of linearly active S-boxes for the first 32 rounds as in the following table.

r	5	6	7	8	9	10	11
m_r	1	1	2	6	6	7	7
r	12	13	14	15	16	17	18
m_r	8	9	13	14	16	17	17
r	19	20	21	22	23	24	25
m_r	18	18	19	19	20	24	24
r	26	27	28	29	30	31	32
m_r	25	25	26	27	31	32	34

In this table, r and m_r denote the round number and the minimum active number respectively.

In this paper, we give a further discussion on this structure. Firstly, we reduce the problem to one about matrices of state transition probabilities. Then, we "spones" matrices ("spones" means replacing all nonzero elements in a matrix by 1. See section 4 for details.) so that we get transition character matrices and their recursive relations. Finally, by further "spones", we get a sequence of active numbers, from which the minimum active number could be obtained. Following this idea, we present a general formula for calculating $LLESA_r$, the minimum numbers of linearly active S-boxes for arbitrary r rounds (see Definition 2.6. Note that the minimum number here means a low bound that can be achieved.). More precisely, we proved that if the round number $r \geq 5$, then

$$LLESA_r = LLESA_{5+((r-5) \bmod 16)} + 18[\frac{r-5}{16}],$$

where the symbol [ ] denotes the integral part of an integer.

In sum, we have solved the problem of describing the ability and the effectiveness for block ciphers, whose key embeddings are based only on the operator $\oplus$, to resist linear analyses and differential analyses.

We should mention that the first version of this paper, in which the key ideas of the present paper are included, was completed in 2006.

2 Description of linear spread values

Let $F : \mathbf{F}_2^e \to \mathbf{F}_2^e$ be a transformation. For any $w, v \in \mathbf{F}_2^e$, if $X \in \mathbf{F}_2^e$ is an identically distributed random variable, we define the mathematical expectation:

$$E((-1)^{wX \oplus vF(X)}) = \frac{1}{2^e} \sum_{X \in \mathbf{F}_2^e} (-1)^{wX \oplus vF(X)}.$$

Obviously,

$$E((-1)^{wX \oplus vF(X)}) == \begin{cases} 1 & \text{if } w = v = 0, \\ 0 & \text{if only one of } w, v \text{ is zero.} \end{cases}$$

Definition 2.1 For any $w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}, v_0, v_1, \cdots, v_{r-1}, w_{r,1}, w_{r,2}, w_{r,3}, w_{r,4} \in \mathbf{F}_2^{32}$, let

$$\iota_r := (w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}, v_0, v_1, \cdots, v_{r-1}, w_{r,1}, w_{r,2}, w_{r,3}, w_{r,4}),$$

and define

$$\varphi_r := \varphi_r(w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}, v_0, v_1, \cdots, v_{r-1}, w_{r,1}, w_{r,2}, w_{r,3}, w_{r,4})$$

$$= \sum_{i=1}^{4} w_{0,i} X_{0,i} \oplus \sum_{i=0}^{r-1} v_i K_i \oplus \sum_{i=1}^{4} w_{r,i} X_{r,i},$$

where $X_{0,i}, K_i, X_{r,i} \in \mathbf{F}_2^{32}$. The vector ι_r is called *the r-round linear spread locus*, the mathematical expectation $\overline{E}(\varphi_r) := E((-1)^{\varphi_r})$ *the r-round linear spread value of* ι_r and $L_{\overline{CP}} := \max\{|\overline{E}(\varphi_r)| < 1\}$ *the r-round maximum linear spread value,* where

$$E((-1)^{\varphi_r}) = \frac{1}{2^{32(r+4)}} \sum_{X_{0,1},\ldots,X_{0,4};K_0,\ldots,K_{r-1}\in\mathbf{F}_2^{32}} (-1)^{\sum_{i=1}^{4} w_{0,i}X_{0,i} \oplus \sum_{i=0}^{r-1} v_i K_i \oplus \sum_{i=1}^{4} w_{r,i}X_{r,i}}.$$

Lemma 2.2: Let $Y_t = X_{t,4} \oplus K_t, t \geq 0$. Then

$$\begin{aligned}
\varphi_1 &= (w_{0,1} \oplus w_{1,2})X_{0,1} \oplus (w_{0,2} \oplus w_{1,3})X_{0,2} \oplus (w_{0,3} \oplus w_{1,4})X_{0,3} \\
&\quad \oplus (w_{0,4} \oplus w_{1,1} \oplus v_0)X_{0,4} \oplus v_0 Y_0 \oplus w_{1,4}F(Y_0); \\
\varphi_{r+1} &= \varphi_r(w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}, v_0, v_1, \cdots, v_{r-1}, w_{r+1,2}, w_{r+1,3}, w_{r+1,4}, w_{r+1,1} \oplus v_r) \\
&\quad \oplus v_r Y_r \oplus w_{r+1,4}F(Y_r).
\end{aligned}$$

Proof: We have

$$\begin{aligned}
\varphi_1 &= \sum_{l=1}^{4} w_{0,l}X_{0,l} \oplus \sum_{t=0}^{1-1} v_t K_t \oplus \sum_{l=1}^{4} w_{1,l}X_{1,l} \\
&= \sum_{l=1}^{4} w_{0,l}X_{0,l} \oplus v_0 K_0 \oplus w_{1,1}X_{0,4} \oplus w_{1,2}X_{0,1} \\
&\quad \oplus w_{1,3}X_{0,2} \oplus w_{1,4}(X_{0,3} \oplus F(X_{0,4} \oplus K_0)) \\
&= (w_{0,1} \oplus w_{1,2})X_{0,1} \oplus (w_{0,2} \oplus w_{1,3})X_{0,2} \oplus (w_{0,3} \oplus w_{1,4})X_{0,3} \\
&\quad \oplus (w_{04,} \oplus w_{1,1})X_{0,4} \oplus v_0(X_{0,4} \oplus K_0) \oplus v_0 X_{0,4} \oplus w_{1,4}F(X_{0,4} \oplus K_0) \\
&= (w_{0,1} \oplus w_{1,2})X_{0,1} \oplus (w_{0,2} \oplus w_{1,3})X_{0,2} \\
&\quad \oplus (w_{0,3} \oplus w_{1,4})X_{0,3} \oplus (w_{0,4} \oplus w_{1,1} \oplus v_0)X_{0,4} \oplus v_0 Y_0 \oplus w_{1,4}F(Y_0). \\
\varphi_{r+1} &= \sum_{l=1}^{4} w_{0,l}X_{0,l} \oplus \sum_{t=0}^{r} v_t K_t \oplus \sum_{l=1}^{4} w_{r+1,l}X_{r+1,l} \\
&= \sum_{l=1}^{4} w_{0,l}X_{0,l} \oplus \sum_{t=0}^{r} v_t K_t \oplus w_{r+1,1}X_{r,4} \oplus w_{r+1,2}X_{r,1} \\
&\quad \oplus w_{r+1,3}X_{r,2} \oplus w_{r+1,4}(X_{r,3} \oplus F(X_{r,4} \oplus K_r)) \\
&= \sum_{l=1}^{4} w_{0,l}X_{0,l} \oplus \sum_{t=0}^{r-1} v_t K_t \oplus w_{r+1,2}X_{r,1} \oplus w_{r+1,3}X_{r,2} \\
&\quad \oplus w_{r+1,4}X_{r,3} \oplus (w_{r+1,1} \oplus v_r)X_{r,4} \oplus v_r Y_r \oplus w_{r+1,4}F(Y_r) \\
&= \varphi_r(w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}, v_0, v_1, \cdots, v_{r-1}, w_{r+1,2}, w_{r+1,3}, w_{r+1,4}, w_{r+1,1} \\
&\quad \oplus v_r) \oplus v_r Y_r \oplus w_{r+1,4}F(Y_r).
\end{aligned}$$

Lemma 2.3: We have

$$\varphi_r(w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}, v_0, v_1, \cdots, v_{r-1}, w_{r,1}, w_{r,2}, w_{r,3}, w_{r,4})$$

$$
\begin{aligned}
&= (w_{0,1} \oplus w_{r,r\bmod 4+1} \oplus \sum_{j=1}^{[\frac{r}{4}]} v_{4(j-1)+3}) X_{0,1} \\
&\oplus (w_{0,2} \oplus w_{r,(r+1)\bmod 4+1} \oplus \sum_{j=1}^{[\frac{r+1}{4}]} v_{4(j-1)+2}) X_{0,2} \\
&\oplus (w_{0,3} \oplus w_{r,(r+2)\bmod 4+1} \oplus \sum_{j=1}^{[\frac{r+2}{4}]} v_{4(j-1)+1}) X_{0,3} \\
&\oplus (w_{0,4} \oplus w_{r,(r+3)\bmod 4+1} \oplus \sum_{j=1}^{[\frac{r+3}{4}]} v_{4(j-1)}) X_{0,4} \\
&\oplus \sum_{j=0}^{r-1} (v_j Y_j \oplus u_j F(Y_j)),
\end{aligned}
$$

where

$$
u_j = w_{r,((r-j)+2)\bmod 4+1} \oplus \sum_{l=1}^{[\frac{r+2-j}{4}]} v_{4(l-1)+(j+1)},
$$

and the terms are independent of each other.

Proof: This lemma follows from Lemma 2.2 and induction.

Let

$$
\begin{aligned}
v_j &:= (v_{j1}, v_{j2}, v_{j3}, v_{j4}) \in \mathbf{F}_2^{32},\ v_{jk} \in \mathbf{F}_2^8,\ k = 1, 2, 3, 4, \\
u_j &:= (u_{j1}, u_{j2}, u_{j3}, u_{j4}) \in \mathbf{F}_2^{32},\ u_{jk} \in \mathbf{F}_2^8,\ k = 1, 2, 3, 4,
\end{aligned}
$$

and let

$$
\lambda_j := (\lambda_{j1}, \lambda_{j2}, \lambda_{j3}, \lambda_{j4}) = u_j A^T,
$$

where A is the matrix mentioned in the introduction of this paper. Then, we have the following lemmas.

Lemma 2.4:

$$
v_j Y_j \oplus u_j F(Y_j) = \sum_{k=1}^{4} (v_{jk} Y_{jk} \oplus \lambda_{jk} S(Y_{jk})).
$$

Proof: We have

$$
\begin{aligned}
v_j Y_j \oplus u_j F(Y_j) &= v_j Y_j \oplus u_j \cdot (S(Y_{j1}), S(Y_{j2}), S(Y_{j3}), S(Y_{j4}))A \\
&= v_j Y_j \oplus (S(Y_{j1}), S(Y_{j2}), S(Y_{j3}), S(Y_{j4}))A \begin{pmatrix} u'_{j1} \\ u'_{j2} \\ u'_{j3} \\ u'_{j4} \end{pmatrix} \\
&= v_j Y_j \oplus (S(Y_{j1}), S(Y_{j2}), S(Y_{j3}), S(Y_{j4})((u_{j1}, u_{j2}, u_{j3}, u_{j4})A^T)^T \\
&= v_j Y_j \oplus (S(Y_{j1}), S(Y_{j2}), S(Y_{j3}), S(Y_{j4}))(\lambda_{j1}, \lambda_{j2}, \lambda_{j3}, \lambda_{j4})) \\
&= \sum_{k=1}^{4} (v_{jk} Y_{jk} \oplus \lambda_{jk} S(Y_{jk})).
\end{aligned}
$$

Lemma 2.5: Assume that $\overline{E}(\varphi_r) \neq 0$.
i) We have

$$w_{0,1} = w_{r,r\bmod 4+1} \oplus \sum_{j=1}^{[\frac{r}{4}]} v_{4(j-1)+3},$$

$$w_{0,2} = w_{r,(r+1)\bmod 4+1} \oplus \sum_{j=1}^{[\frac{r+1}{4}]} v_{4(j-1)+2},$$

$$w_{0,3} = w_{r,(r+2)\bmod 4+1} \oplus \sum_{j=1}^{[\frac{r+2}{4}]} v_{4(j-1)+1},$$

$$w_{0,4} = w_{r,(r+3)\bmod 4+1} \oplus \sum_{j=1}^{[\frac{r+3}{4}]} v_{4(j-1)},$$

ii) For $j = 0, 1, \cdots, r-1$, we have $v_j = 0$ if and only if $u_j = 0$, where u_j is as defined in Lemma 2.3.

Proof: It follows from Definition 2.1 and Lemma 2.3.

From Lemma 2.5, we know that if $\overline{E}(\varphi_r)$ reaches its maximum value, then the conditions i) and ii) in Lemma 2.5 hold. By the condition i) in Lemma 2.5, we have $\varphi_r = \sum_{j=0}^{r-1}(v_j Y_j \oplus u_j F(Y_j))$, so we have

$$|\overline{E}(\varphi_r)| = |E((-1)^{\sum_{j=0}^{r-1}(v_j Y_j \oplus u_j F(Y_j))})| = |E((-1)^{\sum_{j=0}^{r-1}\sum_{k=1}^{k=4}(v_{jk} Y_{jk} \oplus \lambda_{jk} S(Y_{jk}))})|$$

From the following Definition 2.6, it is easy to see that when the minimum number of linearly active S-boxes of the r-round linear spread locus reaches its minimum value, the value $|\overline{E}(\varphi_r)|$ reaches its maximum value.

For the convenience of analyzing numbers of linearly active S-boxes, we introduce the conception of character as follows.

For any vector $\eta = (\eta_1, \eta_2, \eta_3, \eta_4) \in \mathbf{F}_2^{32}$, with $\eta_1, \eta_2, \eta_3, \eta_4 \in \mathbf{F}_2^8$, the *characters* χ *of* η and of $\eta_l (l = 1, 2, 3, 4)$ are defined respectively by the functions:

$$\chi(\eta) = \begin{cases} 1 & \eta \neq 0, \\ 0 & \eta = 0. \end{cases}$$

and

$$\chi(\eta_l) = \begin{cases} 1 & \eta_l \neq 0, \\ 0 & \eta_l = 0, \end{cases}$$

where $l = 1, 2, 3, 4$.

We call the vector $(\chi(\eta_1), \chi(\eta_2), \chi(\eta_3), \chi(\eta_4))$ *the subcharacter of* η.

Definition 2.6: Let $w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}, v_0, v_1, \cdots, v_{r-1}, w_{r,1}, w_{r,2}, w_{r,3}, w_{r,4} \in \mathbf{F}_2^{32}$, and

$$\iota_r = (w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}, v_0, v_1, \cdots, v_{r-1}, w_{r,1}, w_{r,2}, w_{r,3}, w_{r,4}).$$

Assume that

i) $w_{0,1}, w_{0,2}, w_{0,3}, w_{0,4}$are not all zero;

ii) $v_0, v_1, \cdots, v_{r-1}$ are not all zero;

iii) $w_{r,1}, w_{r,2}, w_{r,3}, w_{r,4}$ are not all zero;

iv) $v_{jl} = 0$ if and only if $\lambda_{jl} = 0$, where

$$v_j := (v_{j1}, v_{j2}, v_{j3}, v_{j4}) \in \mathbf{F}_2^{32},\ v_{jk} \in \mathbf{F}_2^8,\ k = 1, 2, 3, 4,$$

$$\lambda_j := (\lambda_{j1}, \lambda_{j2}, \lambda_{j3}, \lambda_{j4}) := \left(w_{r,((r-j)+2)\bmod 4+1} \oplus \sum_{l=1}^{[\frac{r+2-j}{4}]} v_{4(l-1)+(j+1)} \right) A^T.$$

Then, the value $LESA_r(\iota_r) = \sum_{j=0}^{r-1} \sum_{l=1}^{4} \chi(v_{jl})\chi(\lambda_{jl})$ is defined to be the *number of linearly active S-boxes of the r-round linear spread locus*, and the value $LLESA_r = \min_{\iota_r}(LESA_r(\iota_r) > 0)$ is defined to be the *minimum number of linearly active S-boxes of the r-round linear spread locus.*

Clearly, the word minimum here means the minimum number, that is, a low bound that can be achieved.

3 The minimum number of linearly active S-boxes

For any $a_j, b_j \in \mathbf{F}_2^{32}, j = 0, 1, \cdots, r-1$, we have the set of equations (E) about $v_0, v_1, \cdots, v_{r-1}$, $w_{r,1}, w_{r,2}, w_{r,3}, w_{r,4}$ under the condition that $\overline{E}(\varphi_r) \neq 0$ as follows.

$$(E) \begin{cases} v_j = a_j, \\ w_{r,(r+2-j)\bmod 4+1} \oplus \sum_{t=1}^{[\frac{r+2-j}{4}]} v_{4(t-1)+j+1} = b_j, \end{cases}$$

where $j = 0, 1, \cdots, r-1$.

Now, let

$$a_j := (a_{j1}, a_{j2}, a_{j3}, a_{j4}) \in \mathbf{F}_2^{32},\ a_{jk} \in \mathbf{F}_2^8,\ k = 1, 2, 3, 4,$$
$$b_j := (b_{j1}, b_{j2}, b_{j3}, b_{j4}) \in \mathbf{F}_2^{32},\ b_{jk} \in \mathbf{F}_2^8,\ k = 1, 2, 3, 4,$$
$$c_j = (c_{j1}, c_{j2}, c_{j3}, c_{j4}) = b_j A^{\mathrm{T}}.$$

Then we have:

Lemma 3.1: The equations (E) is solvable if and only if

$$c_j \oplus a_{j+1}A^T = c_{j+4}, \quad j = 0, 1, \cdots, r-4.$$

Proof: We have the following computation:

$$b_j = w_{r,((r-j)+2)\bmod 4+1} \oplus \sum_{l=1}^{[\frac{r+2-j}{4}]} a_{4(l-1)+(j+1)},$$

$$b_{j+4} = w_{r,((r-j-4)+2)\bmod 4+1} \oplus \sum_{l=1}^{[\frac{r+2-j-4}{4}]} a_{4(l-1)+(j+4+1)}$$

$$= w_{r,((r-j)+2)\bmod 4+1} \oplus \sum_{l=1}^{[\frac{r+2-j}{4}-1]} a_{4l+(j+1)}$$

$$= w_{r,((r-j)+2)\mathrm{mod}4+1} \oplus \sum_{l=2}^{[\frac{r+2-j}{4}]} a_{4(l-1)+(j+1)}$$

$$= w_{r,((r-j)+2)\mathrm{mod}4+1} \oplus \sum_{l=1}^{[\frac{r+2-j}{4}-1]} a_{4(l-1)+(j+1)}) \oplus a_{j+1}$$

$$= b_j \oplus a_{j+1} = c_j (A^T)^{-1} \oplus a_{j+1},.$$

So we have

$$c_{j+4} = b_{j+4}A^{\mathrm{T}} = c_j \oplus a_{j+1}A^{\mathrm{T}}.$$

Hence, the number of linearly active S-boxes of the r-round linear spread locus ι_r can be written as:

$$LESA_r(\iota_r) = \sum_{j=0}^{r-1}\sum_{l=1}^{4} \chi(a_{jl})\chi(c_{jl}),$$

where a_j, c_j satisfies $c_j \oplus a_{j+1}A^T = c_{j+4}$.

Obviously, $\chi(a_{jl})\chi(c_{jl}) = 0$ when $\chi(a_{jl}) \neq \chi(c_{jl})$. So, to obtain $LESA_r(\iota_r)$, it suffices to calculate $\sum_{j=0}^{r-1}\sum_{l=1}^{4} \chi(v_{jl})\chi(\lambda_{jl})$ under the conditions: $c_j \oplus a_{j+1}A^{\mathrm{T}} = c_{j+4}$ and $\chi(a_{jl}) = \chi(c_{jl})$.

For a vector $X = (x_1, x_2, ..., x_e) \in \mathbf{F}_2^e$, the number of nonzero $x_i (i = 1, 2, ..., e)$ is called the *weight* of X, denoted by $W_H(X)$. For any vector $\eta = (\eta_1, \eta_2, \eta_3, \eta_4) \in \mathbf{F}_2^{32}$, with $\eta_1, \eta_2, \eta_3, \eta_4 \in \mathbf{F}_2^8$, we write

$$w(\eta) := W_H(\chi(\eta_1), \chi(\eta_2), \chi(\eta_3), \chi(\eta_4)).$$

Clearly, $w(\eta)$ can be regarded as an element of $\mathbf{F}_5$.

Lemma 3.2: Let $a_j = (a_{j1}, a_{j2}, a_{j3}, a_{j4})$, $a_{jk} \in \mathbf{F}_2^8, j = 0, 1, 2, ..., r-4; k = 1, 2, 3, 4$. If $\chi(a_{jl}) = \chi(c_{jl})$ and $c_j \oplus a_{j+1}A^T = c_{j+4}$, $j = 0, 1, \cdots, r-4$, then

$$LESA_r(\iota_r) = \sum_{j=0}^{r-1}\sum_{l=1}^{4} \chi(a_{jl}) = \sum_{j=0}^{r-1} w(a_j).$$

Proof: Clear.

From Lemma 3.2, to obtain $LESA_r(\iota_r)$, it suffices to calculate $\sum_{j=0}^{r-1} w(a_j)$ under the conditions $\chi(a_{jl}) = \chi(c_{jl})$ and $c_j \oplus a_{j+1}A^T = c_{j+4}$, $j = 0, 1, \cdots, r-4$. At first, let us analysis the case of the fifth round. In this case, we need to know that in the sequence $w(a_0), w(a_1), w(a_2), w(a_3), w(a_4)$, how the number $w(a_4)$ is depended on $w(a_0)$ and $w(a_1)$. This is given in the following two lemmas.

Lemma 3.3: (1) If $w(a_j) = 0$, then $w(a_jA^{\mathrm{T}}) = 0$.

(2) If $w(a_j) = 1$, then $w(a_jA^{\mathrm{T}}) = 4$.

(3) If $w(a_j) = 2$, then $w(a_jA^{\mathrm{T}}) = 3$ or 4.

(4) If $w(a_j) = 3$, then $w(a_jA^{\mathrm{T}}) = 2, 3$ or 4.

(5) If $w(a_j) = 4$, then $w(a_jA^{\mathrm{T}}) = 1, 2, 3$ or 4.

Proof: It can be checked by computer.

In the case of the fifth round, we have the sequence $w(a_0), w(a_1), w(a_2), w(a_3), w(a_4)$.

Lemma 3.4: The relations between $w(a_0), w(a_1)$ and $w(a_4)$ are shown in the following table.

$w(a_0)$	$w(a_1)$	$w(a_4)$	$w(a_0)$	$w(a_1)$	$w(a_4)$
0	0	0	2	3	0,1,2,3 or 4
0	1	4	2	4	0,1,2,3 or 4
0	2	3 or 4	3	0	3
0	3	2,3 or 4	3	1	1,2,3 or 4
0	4	1,2,3 or 4	3	2	0,1,2,3 or 4
1	0	1	3	3	0,1,2,3 or 4
1	1	3 or 4	3	4	0,1,2,3 or 4
1	2	2,3 or 4	4	0	4
1	3	1,2,3 or 4	4	1	0,1,2,3 or 4
1	4	0,1,2,3 or 4	4	2	0,1,2,3 or 4
2	0	2	4	3	0,1,2,3 or 4
2	1	2,3 or 4	4	4	0,1,2,3 or 4
2	2	1,2,3 or 4			

Proof: It can be checked by computer.

Since $w(a_j) \in \mathbf{F}_5$, there are 624×624 cases of state transitions from $w(a_0), w(a_1), w(a_2), w(a_3)$ to $w(a_0), w(a_1), w(a_2), w(a_3), w(a_4)$. By Lemma 3.4, these state transitions can be expressed by five 624×624 matrices.

4 The recurrent formula for the minimum numbers of linearly active S-boxes

Let $a_0, a_1, \cdots, a_{l-1}$ be a sequence satisfying the condition

$$\chi(a_{jl}) = \chi(c_{jl}), \quad c_j \oplus a_{j+1}A^T = c_{j+4}.$$

Then we have the corresponding sequence $w(a_0), w(a_1), \ldots, w(a_{l-1})$. For convenience, we let $\tau_k := w(a_k), k = 0, 1, ..., l-1$. So, we have a sequence:

$$\tau_0, \tau_1, \ldots, \tau_{l-1}. \qquad (*)$$

Define the following two functions:

$$w(\tau_0, \tau_1, \ldots, \tau_{l-1}) := \tau_0 + \tau_1 + \ldots + \tau_{l-1},$$

$$\varrho(\tau_{l-4}, \tau_{l-3}, \tau_{l-2}, \tau_{l-1}) := \tau_{l-4} \cdot 5^3 + \tau_{l-3} \cdot 5^2 + \tau_{l-2} \cdot 5 + \tau_{l-1}.$$

If $\varrho(\tau_{l-4}, \tau_{l-3}, \tau_{l-2}, \tau_{l-1}) = j$, we call $\tau_{l-4}, \tau_{l-3}, \tau_{l-2}, \tau_{l-1}$ *the final state* of the sequence $(*)$, briefly, we call j the final state of $(*)$.

For any integers i, j satisfying $1 \le i, j \le 624$, if $i = \tau_{l-5}\tau_{l-4}\tau_{l-3}\tau_{l-2}, j = \tau_{l-4}\tau_{l-3}\tau_{l-2}\tau_{l-1}$ as 5-adic numbers and if $\tau_{l-5}\tau_{l-4}$ and τ_{l-1} satisfy the relations in Lemma 3.4, then we say that there is a state transition relation T from $\tau_{l-5}\tau_{l-4}\tau_{l-3}\tau_{l-2}$ to $\tau_{l-4}\tau_{l-3}\tau_{l-2}\tau_{l-1}$, or, we say that there is a state transition relation T from i to j.

In order to express the sum of weight $w(\tau_0, \tau_1, \ldots, \tau_{l-1})$ of the sequence (*), we construct a $(0, 1)$-matrix of 624×624 order as follows.

$$H_l := (H_{lj}[i]),$$

where i and j are the subscripts of rows and columns respectively, and in which for any $1 \leq i, j \leq 624$,

$H_{lj}[i] = 1 \iff$ there exists a sequence (*) with final state j such that $w(\tau_0, \tau_1, \ldots, \tau_{l-1}) = i$.

Clearly, this implies that for any $H_{lj}[i]$ with $1 \leq i, j \leq 624$, we have

$$w(\tau_0, \tau_1, \ldots, \tau_{l-1}) = i, \quad \varrho(\tau_{l-4}, \tau_{l-3}, \tau_{l-2}, \tau_{l-1}) = j.$$

Obviously, the row subscript of the first nonzero row of H_l is just $LLESA_r$.

Now, we turn to see what happens for numbers of linearly active S-box when $\tau_0, \tau_1, \ldots, \tau_{l-1}$ is transferred to $\tau_0, \tau_1, \ldots, \tau_{l-1}, \tau_l$.

At first, we construct five $(0,1)$-matrix of order 624 C_0, C_1, C_2, C_3 and C_4 as follows. Let

$$C_k := (C_k(i,j)), \quad k = 0, 1, 2, 3, 4,$$

in which for any $1 \leq i, j \leq 624$,

$$C_k(i,j) = 1 \iff j \equiv k (\mathrm{mod}\, 5) \text{ and } i, j \text{ have state transition relation } T.$$

See Appendix for the generating algorithm of the matrices C_0, C_1, C_2, C_3 and C_4. (This program is realized by the matlab language.)

Obviously, the columns of C_k are all zero except the column $k \equiv j (\mathrm{mod}\ 5)$.

Since the matrix H_l can be obtained from H_4 by recurrent method, we now turn to the generation of H_4.

I. Generation of H_4

(1) Take H_4 to be the 624×624 zero matrix.

(2) For any 10-adic integer j $(1 \leq j \leq 624)$, write j as a 5-adic integer with 4-digits, that is, $j = \tau_0\tau_1\tau_2\tau_3$.

(3) Calculate the value $w(\tau_0, \tau_1, \tau_2, \tau_3)$, say, $w(\tau_0, \tau_1, \tau_2, \tau_3) = i$.

(4) Put the number 1 on the position (i, j) of H_4.

II. Generating H_5 from H_4

For a matrix $A = (a_{ij})$, we use the symbol spones(A) to denote the matrix (a'_{ij}), where

$$a'_{ij} = \begin{cases} 1 & \text{if } a_{ij} \neq 0, \\ 0 & \text{if } a_{ij} = 0, \end{cases}$$

that is, replace all nonzero elements of A by the number 1.

We will use the symbol $H_l[i]$ to denote the i-th row vector of the matrix H_l.

Lemma 4.1. For any integer i, j $(1 \leq i, j \leq 624)$, let $j = \tau_1\tau_2\tau_3\tau_4$ as a 5-adic integer. Suppose that

$$\mathrm{spones}(H_4[i-k]C_k) = (h_{i-k,1},\ h_{i-k,2},\ ...,\ h_{i-k,624}),\ \ i-k \geq 1,\ \ k = 0, 1, 2, 3, 4.$$

Then, we have

(1) if $j \neq k (\mathrm{mod} 5)$, then $h_{i-k,j} = 0$;

(2) if $j \equiv k (\mathrm{mod} 5)$, i.e., $\tau_4 = k$, then $h_{i-k,j} = 1$ if and only if there exists $t = \varrho(\tau_0, \tau_1, \tau_2, \tau_3)$ such that there exists a state transition relation T from t to j and $w(\tau_0, \tau_1, \tau_2, \tau_3, \tau_4) = i$.

Proof: For $k = 0, 1, 2, 3, 4$, we have

$$H_4[i-k]C_k = (H_{4,1}[i-k], H_{4,2}[i-k], ..., H_{4,624}[i-k])C_k$$

$$= (\sum_{t=1}^{624} H_{4,t}[i-k]C_k(t,1), \sum_{t=1}^{624} H_{4,t}[i-k]C_k(t,2), ..., \sum_{t=1}^{624} H_{4,t}[i-k]C_k(t,624)).$$

(1) Trivial.

(2) When $j \equiv k (\mathrm{mod}\, 5)$, we have

$$\mathrm{spones}(\sum_{t=1}^{624} H_{4,t}[i-k]C_k(t,j)) = 1 \Longleftrightarrow \text{there exists a } t \text{ such that } H_{4,t}[i-k]C_k(t,j) = 1,$$

while we have

$$C_k(t,j) = 1 \Longleftrightarrow \text{there exists a state transition relation } T \text{ from } t \text{ to } j,$$

$$H_{4,t}[i-k] = 1 \Longleftrightarrow w(\tau_0,\tau_1,\tau_2,\tau_3) = i-k \Longleftrightarrow w(\tau_0,\tau_1,\tau_2,\tau_3,\tau_4) = i.$$

Hence, we have

$$\mathrm{spones}(\sum_{t=1}^{624} H_{4,t}[i-k]C_k(t,j)) = 1$$

if and only if there exists $t = \varrho(\tau_0,\tau_1,\tau_2,\tau_3)$ such that there exists a state transition relation T from t to j and $w(\tau_0,\tau_1,\tau_2,\tau_3,\tau_4) = i$.

Lemma 4.2. We have

$$H_5[i] = \mathrm{spones}(H_4[i]C_0 + H_4[i-1]C_1 + H_4[i-2]C_2 + H_4[i-3]C_3 + H_4[i-4]C_4).$$

For $k = 1, 2, 3, 4$, if $i - k \leq 0$, we assume that $H_4[i-k] = 0$ is a row of zeros.

Proof We have $H_5[i] = (H_{5,1}[i], H_{5,2}[i], ..., H_{5,624}[i])$. Write

$$\mathrm{spones}(H_4[i-k]C_k) = (h_{i-k,1},\ h_{i-k,2}, ...,\ h_{i-k,624})$$

as in Lemma 4.1.

Form Lemma 4.1, if $j \bmod 5 \neq k$, then $h_{i-k,j} = 0$; if $j \bmod 5 = k (\tau_4 = k)$, from the definition we know

$$\begin{aligned} H_{5j}[i] = 1 &\Longleftrightarrow \text{ there exist } \tau_0,\tau_1,\tau_2,\tau_3,\tau_4 \text{ with final state } j \text{ such that } w(\tau_0,\tau_1,\tau_2,\tau_3,\tau_4) = i \\ &\Longleftrightarrow \text{ there exist } \tau_0,\tau_1,\tau_2,\tau_3,\tau_4 \text{ such that } \varrho(\tau_0,\tau_1,\tau_2,\tau_3) = t \text{ with a state} \\ &\qquad \text{transition relation } T \text{ from } t \text{ to } j \text{ and } w(\tau_0,\tau_1,\tau_2,\tau_3,\tau_4) = i \\ &\Longleftrightarrow \ h_{i-k,j} = 1, \end{aligned}$$

which means that if $j \bmod 5 = k (\tau_4 = k)$, we have $H_{5j}[i] = h_{i-k,j}$.

So, we obtain

(1) $H_5[i]$ and $\mathrm{spones}(H_4[i]C_0)$ have same elements on the columns 0 (mod 5), and the other elements of $\mathrm{spones}(H_4[i]C_0)$ are all zero.

(2) $H_5[i]$ and $\mathrm{spones}(H_4[i-1]C_1)$ have same elements on the columns 1 (mod 5), and the other elements of $\mathrm{spones}(H_4[i-1]C_1)$ are all zero.

(3) $H_5[i]$ and $\mathrm{spones}(H_4[i-2]C_2)$ have same elements on the columns 2 (mod 5), and the other elements of $\mathrm{spones}(H_4[i-2]C_2)$ are all zero.

(4) $H_5[i]$ and $\mathrm{spones}(H_4[i-3]C_3)$ have same elements on the columns 3 (mod 5), and the other elements of $\mathrm{spones}(H_4[i-3]C_3)$ are all zero.

(5) $H_5[i]$ and spones$(H_4[i-4]C_4)$ have same elements on the columns 4 (mod 5), and the other elements of spones$(H_4[i-4]C_4)$ are all zero.

Hence, we have

$$H_5[i] = \text{spones}(H_4[i]C_0) + \text{spones}(H_4[i-1]C_1) + \text{spones}(H_4[i-2]C_2) + \text{spones}(H_4[i-3]C_3)$$
$$+\text{spones}(H_4[i-4]C_4)$$
$$= \text{spones}(H_4[i]C_0 + H_4[i-1]C_1 + H_4[i-2]C_2 + H_4[i-3]C_3 + H_4[i-4]C_4).$$

Now, from H_4 and Lemma 4.2, we get H_5.

Similarly, we have

Lemma 4.3. We have

$$H_{l+1}[i] = \text{spones}(H_l[i]C_0 + H_l[i-1]C_1 + H_l[i-2]C_2 + H_l[i-3]C_3 + H_l[i-4]C_4).$$

For $k = 1, 2, 3, 4$, if $i - k \leq 0$, we assume that $H_l[i-k] = 0$ is a row of zeros.

From Lemma 4.3 and H_4, we can get H_r, then find out the row subscript m_r corresponding the first nonzero row in H_r, and hence obtain the minimum active number m_r of S-boxes.

Lemma 4.4: The minimum numbers of linearly active S-boxes of the first 52 rounds linear spread locus are as follows.

r	5	6	7	8	9	10	11	12	13	14	15	16
m_r	1	1	2	6	6	7	7	8	9	13	14	16
r	17	18	19	20	21	22	23	24	25	26	27	28
m_r	17	17	18	18	19	19	20	24	24	25	25	26
r	29	30	31	32	33	34	35	36	37	38	39	40
m_r	27	31	32	34	35	35	36	36	37	37	38	42
r	41	42	43	44	45	46	47	48	49	50	51	52
m_r	42	43	43	44	45	49	50	52	53	53	54	54

where r and m_r denote the round number and the minimum active number respectively.

Proof: By computer.

From the table in Lemma 4.4, we know that for every 16 rounds, the minimum numbers of linearly active S-boxes increase by 18. Iterating 15 times the formula

$$H_{l+1}[i] = \text{spones}(H_l[i]C_0 + H_l[i-1]C_1 + H_l[i-2]C_2 + H_l[i-3]C_3 + H_l[i-4]C_4),$$

we get

$$H_{l+16}[i] = \text{spones}(H_l[i]A_0 + H_l[i-1]A_1 + \cdots + H_l[i-64]A_{64}),$$

where $A_0, A_1, \cdots, A_{64}$ are all $0,1$ matrix of order 624 (The matrices $A_0, A_1, \cdots, A_{64}$ can be obtained by computer). Calculating by computer, we know that $A_0, A_1, \cdots, A_{15}$ are all zero matrix. Hence, we have:

Lemma 4.5: If $i - k \leq 0$, let $H_l[i-k] = 0$(zero row). Then

$$H_{l+16}[i] = \text{spones}(H_l[i-16]A_{16} + H_l[i-17]A_{17}$$
$$+ \cdots + H_l[i-64]A_{64}).$$

Lemma 4.6: Let m_l denote the row subscript of the first nonzero row of H_l. Then

(1) the first $m_l + 15$ rows of H_{l+16} are all zero.

(2) $H_{l+16}[m_l + 16] = \text{spones}(H_l[m_l]A_{16})$.

(3) $H_{l+16}[m_l + 17] = \text{spones}(H_l[m_l + 1]A_{16} + H_l[m_l]A_{17})$.

(4) $H_{l+16}[m_l + 18] = \text{spones}(H_l[m_l + 2]A_{16} + H_l[m_l + 1]A_{17} + H_l[m_l]A_{18})$.

Proof: (1) When $1 \leq k \leq 15$, $(m_l + k) - 16 < m_l$, so

$$H_l[(m_l + k) - 16] = H_l[(m_l + k) - 17] = \cdots$$

$$= H_l[(m_l + k) - 64] = 0.$$

Hence, form Lemma 4.5, we have $H_{l+16}[m_l + k] = 0$, that is, the first $m_l + 15$ rows of H_{l+16} are all zero.

(2) We have

$$H_{l+16}[m_l + 16] = \text{spones}(H_l[m_l]A_{16} + H_l[m_l - 1]A_{17} +$$

$$\cdots + H_l[m_l - 48]A_{64}).$$

Since $H_l[m_l-1] = H_l[m_l-2] = \cdots = H_l[m_l-48] = 0$, we get $H_{l+16}[m_l+16] = \text{spones}(H_l[m_l]A_{16})$.

Similarly for (3)(4).

When $l > 20$, write $l = u + 16k$, $u = 5, 6, \cdots, 20$. If the first nonzero row of H_{u+16k} is the $m_u^{(k)}$-th row, then the equalities in Lemma 4.6 can be written as:

$$H_{u+16(k+1)}[m_u^{(k)} + 16] = \text{spones}(H_{u+16k}[m_u^{(k)}]A_{16}),$$

$$H_{u+16(k+1)}[m_u^{(k)} + 17] = \text{spones}(H_{u+16k}[m_u^{(k)} + 1]A_{16}$$

$$+H_{u+16k}[m_u^{(k)}]A_{17}),$$

$$H_{u+16(k+1)}[m_u^{(k)} + 18] = \text{spones}(H_{u+16k}[m_u^{(k)} + 2]A_{16}$$

$$+H_{u+16k}[m_u^{(k)} + 1]A_{17} + H_{u+16k}[m_u^{(k)}]A_{18}).$$

Lemma 4.7: The matrices A_i obtained above satisfy

(1) $A_{16}A_{16} = A_{16}A_{17} = A_{17}A_{16} = A_{16}A_{18} = A_{16}A_{19} = 0$.

(2) $A_{18}A_{16} = A_{19}A_{16} = A_{20}A_{16} = A_{17}A_{17} = A_{16}$.

(3) $\text{spones}(A_{18}^3) = \text{spones}(A_{18}^2)$.

(4) $\text{spones}(A_{17}A_{18}A_{17}) = \text{spones}(A_{16} + A_{16}P)$, where $A_{16}P$ is the matrix obtained by exchanging the 25-th column and the 500-th column of A_{16}.

(5) $\text{spones}(A_{18}A_{18}A_{17}) = \text{spones}(A_{18}A_{17})$.

Proof: By computer.

Lemma 4.8: For $u = 5, 6, \cdots, 20$, if $m_u^{(t)} = m_u^{(t-1)} + 18$, then

(1) $H_{u+16(t-1)}[m_u^{(t-1)}]A_{16} = 0$.

(2) $H_{u+16(t-1)}[m_u^{(t-1)} + 1]A_{16} = 0$, $\quad H_{u+16(t-1)}[m_u^{(t-1)}]A_{17} = 0$.

(3) $\text{spones}(H_{u+16t}[m_u^{(t)}]A_{18}A_{17}) = \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{17})$.

Proof: (1) Since

$$H_{u+16t}[m_u^{(t-1)} + 16] = \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}]A_{16})$$

and $m_u^{(t)} = m_u^{(t-1)} + 18$, we have $H_{u+16t}[m_u^{(t-1)} + 16] = 0$, that is $H_{u+16(t-1)}[m_u^{(t-1)}]A_{16} = 0$.

(2) Since

$$H_{u+16t}[m_u^{(t-1)} + 17] = \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)} + 1]A_{16}$$

$$+H_{u+16(t-1)}[m_u^{(t-1)}]A_{17})$$

and $m_u^{(t)} = m_u^{(t-1)} + 18$, we have $H_{u+16t}[m_u^{(t-1)} + 17] = 0$, so

$$H_{u+16(t-1)}[m_u^{(t-1)} + 1]A_{16} = 0,$$

$$H_{u+16(t-1)}[m_u^{(t-1)}]A_{17} = 0.$$

(3) We have

$$\begin{aligned}
\text{spones}(H_{u+16t}[m_u^{(t)}]A_{18}A_{17}) &= \text{spones}(H_{u+16t}[m_u^{(t-1)}+18]A_{18}A_{17}) \\
&= \text{spones}(\text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+2]A_{16} \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{17} \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}]A_{18})A_{18}A_{17}) \\
&= \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{17}A_{18}A_{17} \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{18}A_{17}) \\
&= \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{16}(I+P) \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{18}A_{17}) \\
&= \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{18}A_{17}) \\
&= \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{17}).
\end{aligned}$$

Lemma 4.9: For $u = 5, 6, \cdots, 20$, if

$$m_u^{(t)} = m_u^{(t-1)} + 18,\ m_u^{(t-1)} = m_u^{(t-2)} + 18,$$

then

(1) $\text{spones}(H_{u+16t}[m_u^{(t)}]A_{16}) = 0$.

(2) $\text{spones}(H_{u+16t}[m_u^{(t)}+1]A_{16}) = 0$.

(3) $\text{spones}(H_{u+16t}[m_u^{(t)}]A_{17}) = \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{17})$.

Proof: (1)

$$\begin{aligned}
\text{spones}(H_{u+16t}[m_u^{(t)}]A_{16}) &= \text{spones}(H_{u+16t}[m_u^{(t-1)}+18]A_{16}) \\
&= \text{spones}(\text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+2]A_{16} \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{17}+H_{u+16(t-1)}[m_u^{(t-1)}]A_{18})A_{16}) \\
&= \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+2]A_{16}A_{16} \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{17}A_{16}+H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{16}). \\
&= \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}]A_{16}) = 0
\end{aligned}$$

(2)

$$\begin{aligned}
\text{spones}(H_{u+16t}[m_u^{(t)}+1]A_{16}) &= \text{spones}(H_{u+16t}[m_u^{(t-1)}+19]A_{16}) \\
&= \text{spones}(\text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+3]A_{16} \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}+2]A_{17}+H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{18} \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}]A_{19})A_{16}) \\
&= \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{18}A_{16} \\
&\quad +H_{u+16(t-1)}[m_u^{(t-1)}]A_{19}A_{16}) \\
&= \text{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{16}+H_{u+16(t-1)}[m_u^{(t-1)}]A_{16}) = 0.
\end{aligned}$$

$$
\begin{aligned}
(3)\ \mathrm{spones}(H_{u+16t}[m_u^{(t)}]A_{17}) &= \mathrm{spones}(H_{u+16t}[m_u^{(t-1)}+18]A_{17}) \\
&= \mathrm{spones}(\mathrm{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+2]A_{16} \\
&\quad + H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{17} + H_{u+16(t-1)}[m_u^{(t-1)}]A_{18})A_{17}) \\
&= \mathrm{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+2]A_{16}A_{17} \\
&\quad + H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{17}A_{17} + H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{17}) \\
&= \mathrm{spones}(H_{u+16(t-1)}[m_u^{(t-1)}+1]A_{16} \\
&\quad + H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{17}) \\
&= \mathrm{spones}(H_{u+16(t-1)}[m_u^{(t-1)}]A_{18}A_{17}).
\end{aligned}
$$

Make all the first non zero rows of $H_u (u = 5, 6, \cdots, 20)$ into the matrix E, all the second nonzero rows into F, and all the third nonzero rows into G.

Write E_k, F_k, G_k for the matrices formed of the first nonzero rows, the second nonzero rows, and the third nonzero rows of $H_{u+16k}, u = 5, 6, \cdots, 20$, respectively.

Lemma 4.10: (1) $EA_{18}A_{17} = 0$.

(2) The nonzero elements of $F_2A_{17}A_{18}A_{18}$ are only at the positions with the subscripts: $(12, 25), (14, 25)$ and $(16, 25)$.

(3) All rows except the 12-th row of $E_2A_{18}A_{18}$ are nonzero. The subscripts of the nonzero elements of $E_2A_{18}A_{18}$ are only as follows.

(1,5),(1,25)
(2,25)
(3,25)
(4,21),(4,25),(4,26),(4,105),(4,129),(4,130),(4,526)
(5,105),(5,130)
(6,26),(6,105),(6,130),(6,526)
(7,130)
(8,26),(8,130)
(9,26)
(10,25),(10,26),(10,46),(10,130),(10,134),(10,155),(10,258),(10,382),(10,506)
(11,25),(11,26),(11,46),(11,155)
(13,5),(13,25),(13,125)
(14,25)
(15,5),(15,25),(15,125)
(16,25)

Proof: It can be checked by computer (by the matlab language).

Theorem 4.11: Let $u = 5, 6, \cdots, 20$. Then for any integer t, we have $m_u^{(t)} = m_u^{(t-1)} + 18$.

Proof: It is true when $t = 1, 2$. Now, assume that when $t = 1, 2, \cdots, k$, we have

$$m_u^{(k)} = m_u^{(k-1)} + 18, m_u^{(k-1)} = m_u^{(k-2)} + 18.$$

From Lemma 4.9, we have

$$H_{u+16(k+1)}[m_u^{(k)} + 16] = \mathrm{spones}(H_{u+16k}[m_u^{(k)}]A_{16}) = 0.$$

So $H_{u+16t}[m_u^{(t-1)} + 16] = 0$.

Now, we have

$$H_{u+16(k+1)}[m_u^{(k)} + 17] = \mathrm{spones}(H_{u+16k}[m_u^{(k)} + 1]A_{16} + H_{u+16k}[m_u^{(k)}]A_{17})$$

$$
\begin{aligned}
&= \text{spones}(H_{u+16k}[m_u^{(k)}]A_{17})\\
&= \text{spones}(H_{u+16k}[m_u^{(k-1)}+18]A_{17})\\
&= \text{spones}(\text{spones}(H_{u+16(k-1)}[m_u^{(k-1)}+2]A_{16}\\
&\quad +H_{u+16(k-1)}[m_u^{(k-1)}+1]A_{17}+H_{u+16(k-1)}[m_u^{(k-1)}]A_{18})A_{17})\\
&= \text{spones}(H_{u+16(k-1)}[m_u^{(k-1)}+2]A_{16}A_{17}\\
&\quad +H_{u+16(k-1)}[m_u^{(k-1)}+1]A_{17}A_{17}+H_{u+16(k-1)}[m_u^{(k-1)}]A_{18}A_{17})\\
&= \text{spones}(H_{u+16(k-1)}[m_u^{(k-1)}+1]A_{16}\\
&\quad +H_{u+16(k-1)}[m_u^{(k-1)}]A_{18}A_{17})\\
&= \text{spones}(H_{u+16(k-1)}[m_u^{(k-1)}]A_{18}A_{17})\\
&= \text{spones}(H_{u+16(k-1)}[m_u^{(k-2)}+18]A_{18}A_{17})\\
&= \text{spones}((H_{u+16(k-2)}[m_u^{(k-2)}+2]A_{16}\\
&\quad +H_{u+16(k-2)}[m_u^{(k-2)}+1]A_{17}+H_{u+16(k-2)}[m_u^{(k-2)}]A_{18})A_{18}A_{17})\\
&= \text{spones}(H_{u+16(k-2)}[m_u^{(k-2)}+1]A_{16}(I+P)\\
&\quad +H_{u+16(k-2)}[m_u^{(k-2)}]A_{18}A_{18}A_{17})\\
&= \text{spones}(H_{u+16(k-2)}[m_u^{(k-2)}]A_{18}A_{17})\\
&\qquad\qquad \cdots\cdots\\
&= \text{spones}(H_u[m_u^{(0)}]A_{18}A_{17}).
\end{aligned}
$$

Since $EA_{18}A_{17}=0$ from Lemma 4.10, we have $H_u[m_u^{(0)}]A_{18}A_{17}=0$. Hence

$$H_{u+16t}[m_u^{(t-1)}+17]=0.$$

Now, let $M_{k+1}=\text{spones}(G_kA_{16}+F_kA_{17}+E_kA_{18})$. From the equality

$$H_{u+16(k+1)}[m_u^{(k)}+18]=\text{spones}(H_{u+16k}[m_u^{(k)}+2]A_{16}+H_{u+16k}[m_u^{(k)}+1]A_{17}+H_{u+16k}[m_u^{(k)}]A_{18}),$$

we have:

$$
\begin{aligned}
M_{k+1} &= \text{spones}(G_kA_{16}+F_kA_{17}+E_kA_{18})\\
&= \text{spones}(G_kA_{16}+F_kA_{17}+\text{spones}(G_{k-1}A_{16}+F_{k-1}A_{17}+E_{k-1}A_{18})A_{18})\\
&= \text{spones}(G_kA_{16}+F_kA_{17}+F_{k-1}A_{17}A_{18}+\text{spones}(E_{k-1}A_{18}A_{18})).
\end{aligned}
$$

Since

$$
\begin{aligned}
\text{spones}(E_{k-1}A_{18}A_{18}) &= \text{spones}((G_{k-2}A_{16}+F_{k-2}A_{17}+E_{k-2}A_{18})A_{18}A_{18})\\
&= \text{spones}(F_{k-2}A_{17}A_{18}A_{18}+E_{k-2}A_{18}A_{18}A_{18})\\
&= \text{spones}(F_{k-2}A_{17}A_{18}A_{18}+E_{k-2}A_{18}A_{18}),
\end{aligned}
$$

recurrently, we have

$$\text{spones}(E_{k-1}A_{18}A_{18})=\text{spones}(F_{k-2}A_{17}A_{18}A_{18}+F_{k-3}A_{17}A_{18}A_{18}+E_{k-3}A_{18}A_{18})$$

$$= \ldots = \text{spones}(F_{k-2}A_{17}A_{18}A_{18} + F_{k-3}A_{17}A_{18}A_{18} + \ldots + F_2A_{17}A_{18}A_{18} + E_2A_{18}A_{18}).$$

Hence,

$$M_{k+1} = \text{spones}(G_kA_{16} + F_kA_{17} + F_{k-1}A_{17}A_{18} + F_{k-2}A_{17}A_{18}A_{18} + F_{k-3}A_{17}A_{18}A_{18} + \ldots + F_2A_{17}A_{18}A_{18} + E_2A_{18}A_{18}).$$

Form Lemma 4.10, we know that all rows of the matrix $F_2A_{17}A_{18}A_{18} + E_2A_{18}A_{18}$ and hence M_{k+1} are nonzero. So, we have proved that $H_{u+16(k+1)}[m_u^{(k)} + 18] \neq 0$ for $u = 5, 6, \ldots, 20$, therefore $H_{u+16t}[m_u^{(t-1)} + 18] \neq 0$, which implies $m_u^{(t)} = m_u^{(t-1)} + 18$, as required.

Theorem 4.12: For any round r, we have

$$LLESA_r = LLESA_{5+((r-5) \bmod 16)} + 18[\frac{r-5}{16}].$$

Proof: For an integer $r \geq 5$, let $u = (r-5) \bmod 16 + 5$ and $t = [\frac{r-5}{16}]$. Then it is easy to see that $r = 16t + u$. Hence

$$LLESA_r = m_u^{(t)}.$$

When $5 \leq r \leq 20$, $t = 0$ and $u = r = ((r-5) \bmod 16) + 5$, so we have

$$LLESA_r = m_u^{(0)} = LLESA_{5+((r-5) \bmod 16)}.$$

When $r > 20$, from Theorem 4.11, we have

$$LLESA_r = m_u^{(t)} = m_u^{(t-1)} + 18 = m_u^{(t-2)} + 36 = \ldots$$

$$= m_u^{(0)} + 18t = LLESA_{5+((r-5) \bmod 16)} + 18[\frac{r-5}{16}].$$

Remarks Although the discussion in this paper focuses on generalized Feistel structures, the our method is suitable to a broad picture. In fact, applying this method to those block ciphers whose key embeddings are based only the operator $\oplus$, such as DES, 3DES, AES, CAST, SMS4, etc., we can give the following results:

(1) We can obtain the explicit formulas for the minimum numbers of both linearly and differentially active S-boxes of arbitrary round.

(2) For different block ciphers and for arbitrary round, using the above explicit formula we can give the comparison of their abilities and effectiveness on resiting linear analysis and differential analysis.

(3) It follows from the similar formula on SMS4 (we will give in another paper) that CAST and SMS4 have the same abilities and effectiveness on resisting linear analyses and differential analyses in any round.

These results will be given in our sequel works.

5 Conclusion

For a class of generalized Feistel block ciphers, we present an explicit recurrent formula for the minimum numbers of linearly active S-boxes of arbitrary rounds, from which we conclude that for every 16 rounds, the minimum numbers of linearly active S-boxes increase by 18.

6 Appendix

```
function ZYJZ
C0=zeros(624);C1=C0;C2=C0;C3=C0;C4=C0;
for k=1:624
  e=dec2base(k,5);
  d=length(e);
  for r=1:d
    m(r)=str2num(e(r));
  end
  if d<4
    m=[zeros(1,4-d),m];
  end
  a=m(1);b=m(2);
  switch a
  case 0
    switch b
    case 0
      c=0;
    case 1
      c=4;
    case 2
      c=[3,4];
    case 3
      c=[2,3,4];
    otherwise
      c=[1:4];
    end
  case a==1
    switch b
    case 0
      c=1;
    case 1
      c=[3,4];
    case 2
      c=[2,3,4];
    case 3
      c=[1,2,3,4];
    otherwise
      c=[0:4];
    end
  case 2
    switch b
    case 0
      c=2;
    case 1
      c=[2:4];
```

```
   case 2
      c=[1:4];
   otherwise
      c=[0:4];
   end
case 3
   switch b
   case 0
      c=3;
   case 1
      c=[1:4];
   otherwise
      c=[0:4];
   end
otherwise
   switch b
   case 0
      c=4;
   otherwise
      c=[0:4];
   end
end
d1=length(c);
f=zeros(d1,4);
f1=zeros(d1,1);
for i=1:d1
   f(i,1:4)=[m(2),m(3),m(4),c(i)];
   f1(i)=c(i)+m(4)*5+m(3)*5^2+m(2)*5^3;
end
switch d1
case 2
   C3(k,f1(1))=1;C4(k,f1(2))=1;
case 3
   C2(k,f1(1))=1;C3(k,f1(2))=1;C4(k,f1(3))=1;
case 4
   C1(k,f1(1))=1;C2(k,f1(2))=1;
   C3(k,f1(3))=1;C4(k,f1(4))=1;
case 5
   C0(k,f1(1))=1;C1(k,f1(2))=1;C2(k,f1(3))=1;
   C3(k,f1(4))=1;C4(k,f1(5))=1;
otherwise
   if a==0&b==0
      C0(k,f1)=1;
   end
   if a==0&b==1
      C4(k,f1)=1;
   end
```

```
        if a==1&b==0
           C1(k,f1)=1;
        end
        if a==2&b==0
           C2(k,f1)=1;
        end
        if a==3&b==0
           C3(k,f1)=1;
        end
        if a==4&b==0
           C4(k,f1)=1;
        end
     end
  end
```

References

[1] Matsui M., Linear cryptanalysis method for DES cipher, *Advances in Cryptology Eurocrypt'93 Proc,Springer-Verlag*, 1994, pp.386-397.

[2] Biham, E.Shamir, A Differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, 1991,4(1),pp.3-72.

[3] Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 461-480. Springer, Heidelberg (1990)

[4] Moriai, S., Vaudenay, S.: On the pseudorandomness of top-level schemes of block ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 289-302. Springer, Heidelberg (2000)

[5] Kim, J., Hong, S., Sung, J., Lee, S., Lim, J., Sung, S.: Impossible differential cryptanalysis for block cipher structures. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 82-96. Springer, Heidelberg (2003)

[6] K. Nyberg and L.R.Knudsen, Provable security against differential cryptanalysis, Advances in Cryptology C CRYPTO92, LNCS 740, pp. 566-574,Springer-Verlag, 1992.

[7] Lee, C., Kim, J., Sung, J., Hong, S., Lee, S.: Provable security for an RC6-like structure and a MISTY-FO-like structure against differential cryptanalysis. In: Gavrilova, M., et al. (eds.) ICCSA 2006. LNCS, vol. 3982, pp. 446-455. Springer, Heidelberg (2006)

[8] Shirai, T., Araki, K.: On generalized Feistel structures using the diffusion switching mechanism. IEICE Trans. Fundamentals E91-A(8), 2120-2129 (2008)

[9] Nyberg, K.: Generalized Feistel network. In: Kim, K., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 91-104. Springer, Heidelberg (1996)

[10] K.Kanda,Practical Security evaluation against differential and linear attacks for Feistel cipher with SPN round function, *SAC'2000 Proc., Berlin, Springer-verlag*, 2000,168-179.

[11] K.Nyberg,L.R.Kundsen,Provable Security Against a Differential Attack, *Journal of Cryptology*, Vol.8,No.1,27-37,1995.

[12] Suzaki, T., Minematsu, K.: Improving the generalized Feistel. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 19-39. Springer, Heidelberg (2010)

[13] Ruwen Zhang, Linear cryptanalysis for a class of generalized Feistel ciphers, *Journal of the Graduate School of the Chinese Academy of Sciences*, 2003, 20(1): 31-38.

[14] Chao Li, Longjiang Qu, and Qiang Li, Differential cryptanalysis of a class of generalized Feistel ciphers, *CHINACRYPT'*2004, 58-63.