On the Security of Generalized Feistel Scheme with SP Round Function

Wenling Wu, Wentao Zhang, and Dongdai Lin
(Corresponding author: Wenling Wu)

State Key Laboratory of Information Security, Institute of Software
Chinese Academy of Sciences, Beijing 100080, P. R. China. (E-mail: wwl@is.iscas.ac.cn)

(Received Sept 9, 2005; revised and accepted Oct. 11, 2005)

Abstract

This paper studies the security against differential/linear cryptanalysis and the pseudorandomness of a class of generalized Feistel scheme with SP round function called $GFSP$. We consider the minimum number of active s-boxes in four, eight and sixteen consecutive rounds of $GFSP$, which provide the upper bound of the maximum differential/linear probabilities of 16-round $GFSP$ scheme, in order to evaluate the strength against differential/linear cryptanalysis. Furthermore, we point out seven rounds $GFSP$ is not pseudorandom for non-adaptive adversary, and prove that eight rounds $GFSP$ is pseudorandom for any adversaries.

Keywords: Branch number, cipher, differential cryptanalysis, linear cryptanalysis, pseudorandomness, S-box.

1 Introduction

The well-known approaches to attack block cipher are differential cryptanalysis proposed by Biham and Shamir [1], and linear cryptanalysis introduced by Matsui [13]. Nyberg [17, 18] first formalized the notion of strength against differential cryptanalysis. Similarly, Chabaud and Vaudenay [2] formalized the notion of strength against linear cryptanalysis. With those notions, we can study how to make a cipher scheme resistant against both attacks. This can be achieved by usual active s-boxes counting tricks. Nyberg and Knudsen [9, 17] gave the upper bounds of differential /linear characteristic probabilities for Feistel scheme by using the minimum numbers of differential/linear active s-boxes. Kanda [7] showed the minimum numbers of differential/linear active s-boxes for Feistel scheme with SP round function. Another approach to study the security of block ciphers was introduced by Luby and Rackoff [11] in 1988. They have shown how to formalize security by pseudorandomness, and how to prove the security of Feistel scheme—provided that round functions are totally random. They showed that three round Feistel scheme is pseudorandom and four round Feistel scheme is super-pseudorandom. Maurer gave a simpler proof for non-adaptive adversaries [14]. Since then, many researchers tried to improve the results and proved the pseudorandomness of other schemes(see, [3, 4, 5, 6, 8, 10, 12, 15, 16, 19, 20, 21, 22, 23]). Among these papers, [23] and [15] have discussed the pseudorandomness of a generalized Feistel scheme called "Type-1 transformation" by Zheng-Matsumoto-Imai and CAST256-like Feistel scheme by Moriai-Vaudenay. They showed that seven round CAST256-like Feistel scheme is pseudorandom. In their paper, they just supposed that round functions are totally random and didn't consider the structure of the round function.

In this paper, we study the security of CAST256-like Feistel scheme with SP round function, which is denoted as $GFSP$ in this paper while the linear transformation P in the round function is fixed and s-boxes are random functions. It is not known yet whether seven round $GFSP$ scheme is pseudorandom and what is the number of rounds that make $GFSP$ scheme pseudorandom. We solve this problem and get the minimum number of active s-boxes in some consecutive rounds of $GFSP$, i.e., in four, eight and sixteen consecutive rounds, which provide the upper bound of the maximum differential/linear probabilities of 16-round $GFSP$ scheme.

This paper is organized as follows: In Section 2, we review the $GFSP$ scheme and definitions. In Section 3, we estimate the upper bounds of differential /linear characteristic probabilities for $GFSP_4$ scheme. Section 4 presents some seven rounds distinguishers for $GFSP$ scheme. In Section 5, the pseudorandomness of $GFSP$ scheme is discussed, and Section 6 concludes the paper.

2 Preliminaries

2.1 $GFSP$ Scheme

This paper we consider type-1 Feistel scheme with $\frac{n}{4}(= ml)$-bit SP round function called $GFSP$ (see Figures 1 and 2). S-function is a non-linear transformation layer

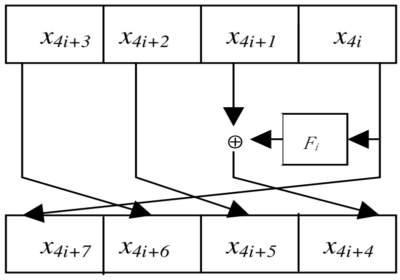

Figure 1: The i-th round transformation

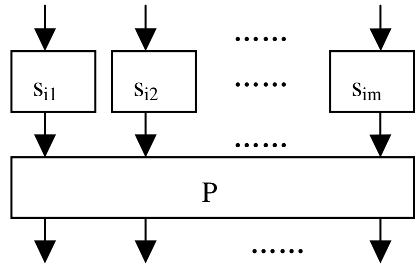

Figure 2: The i-th round function F_i

with m parallel l-bit s-boxes. That is,

$$\begin{aligned} S_i: \quad & (\{0,1\}^l)^m \longrightarrow (\{0,1\}^l)^m \\ & x_j = (x_{j,1},\ldots,x_{j,m}) \\ & \quad \longrightarrow z_j = S_i(x_j) = (s_{i1}(x_{j,1}),\ldots,s_{im}(x_{j,m})). \end{aligned}$$

P-function is a linear transformation layer, which can be defined by a matrix.

$$\begin{aligned} P: \quad & (\{0,1\}^l)^m \longrightarrow (\{0,1\}^l)^m \\ & z_j = (z_{j,1},\ldots,z_{j,m}) \\ & \quad \longrightarrow y_j = P(z_j) = (y_{j,1},\ldots,y_{j,m}). \end{aligned}$$

$$P = \begin{bmatrix} \theta_{11} & \theta_{12} & \cdots & \theta_{1m} \\ \theta_{21} & \theta_{22} & \cdots & \theta_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ \theta_{m1} & \theta_{m2} & \cdots & \theta_{mm} \end{bmatrix}$$

where $\theta_{ij}(1 \le i,j \le m)$ are elements in finite field $GF(2^l)$.

Finally, the ith round function can be described as follows:

$$\begin{aligned} F_i: \quad & (\{0,1\}^l)^m \longrightarrow (\{0,1\}^l)^m \\ & x_j = (x_{j,1},\ldots,x_{j,m}) \\ & \quad \longrightarrow y_j = PS_i(x_j) = P(z_j) = (y_{j,1},\ldots,y_{j,m}). \end{aligned}$$

Let $(x_{4i+3}, x_{4i+2}, x_{4i+1}, x_{4i})$ denote the input of the $(i+1)th$ round. The output of the $(i+1)th$ round of $GFSP$ scheme is defined as:

$$\begin{aligned} x_{4i+4} &= F_i(x_{4i}) \oplus x_{4i+1}, \\ x_{4i+5} &= x_{4i+2}, \\ x_{4i+6} &= x_{4i+3}, \\ x_{4i+7} &= x_{4i+1}. \end{aligned}$$

2.2 Definitions

We use the following definitions in this paper.

Definition 1 *For any given $\triangle x, \triangle z, \Gamma x, \Gamma z \in \{0,1\}^l$, the differential and linear probabilities of each s-boxes are defined as:*

$$\begin{aligned} & DP^s(\triangle x \to \triangle z) \\ & \quad = \frac{|\{x \in \{0,1\}^l | s(x) \oplus s(x \oplus \triangle x) = \triangle z\}|}{2^l} \\ & LP^s(\Gamma z \to \Gamma x) \\ & \quad = (2 \times \frac{|\{x \in \{0,1\}^l | x \cdot \Gamma x = s(x) \cdot \Gamma z\}|}{2^l})^2. \end{aligned}$$

The maximum differential and linear probabilities of s-boxes are defined as:

$$\begin{aligned} p_s &= \max_{ij} \max_{\triangle x \neq 0, \triangle z} DP^{s_{ij}}(\triangle x \to \triangle z) \\ q_s &= \max_{ij} \max_{\Gamma x, \Gamma z \neq 0} LP^{s_{ij}}(\Gamma z \to \Gamma x). \end{aligned}$$

This means that p_s, q_s are the upper bounds of the maximum differential and linear probabilities for all s-boxes.

Definition 2 *A differential active s-box is defined as an s-box given a non-zero input difference, while a linear active s-box is defined as an s-box given a non-zero output mask value.*

Definition 3 *Let $x_i = (x_{i1},\ldots,x_{im}) \in (\{0,1\}^l)^m$, then the Hamming weight of x_i is denoted by*

$$H_w(x_i) = |\{j | x_{i,j} \neq 0\}|.$$

This means that the Hamming weight of x_i equals the number of non-zero l-bit characters from $\{0,1\}^l$ of x_i.

Definition 4 *The branch number P_d of linear transformation $P : (\{0,1\}^l)^m \longrightarrow (\{0,1\}^l)^m$ is defined as:*

$$P_d = \min_{z \neq 0}(H_w(z) + H_w(P(z))).$$

2.3 Pseudorandomness

Let $\mathbf{F}_{n,n}$ denote the set of functions from $\{0,1\}^n$ to $\{0,1\}^n$, A n-bit r-round $GFSP$ scheme $GFSP^{(s_{11},s_{12},\ldots,s_{rm})}$ can be regarded as a random function of $\mathbf{F}_{n,n}$ determined by rm random functions $s_{ij} \in \mathbf{F}_{l,l}, i = 1,\ldots,r, j = 1,\ldots,m$. We define a perfect random function f^* of $\mathbf{F}_{n,n}$ as a uniformly drawn element of $\mathbf{F}_{n,n}$. In other words, f^* is associated with the uniform probability distribution over $\mathbf{F}_{n,n}$. In proof of pseudorandomness of scheme, we want to upper bound the probability of any algorithm to distinguish whether a given fixed function φ is an instance of a random function $f = GFSP^{(s_{11},s_{12},\ldots,s_{rm})}$ of $\mathbf{F}_{n,n}$ or an instance of the perfect random function f^*, using less than q queries to φ.

Let $\mathcal{A}$ be a computationally unbounded distinguisher with an oracle $\mathcal{O}$. The oracle chooses randomly a function φ from $GFSP^{(s_{11},s_{12},\ldots,s_{rm})}$ or $\mathbf{F}_{n,n}$. The aim of the distinguisher $\mathcal{A}$ is to distinguish if the oracle $\mathcal{O}$ implements $GFSP^{(s_{11},s_{12},\ldots,s_{rm})}$ or $\mathbf{F}_{n,n}$. Let p_0 denote the probability that $\mathcal{A}$ outputs 1 when $\mathcal{O}$ implements $\mathbf{F}_{n,n}$, and p_1 denote the probability that $\mathcal{A}$ outputs 1 when $\mathcal{O}$ implements $GFSP^{(s_{11},s_{12},\ldots,s_{rm})}$. That is $p_0 = Pr(\mathcal{A}\ outputs\ 1 \mid \mathcal{O} \leftarrow \mathbf{F}_{n,n})$ and $p_1 = Pr(\mathcal{A}\ outputs\ 1 \mid \mathcal{O} \leftarrow GFSP^{(s_{11},s_{12},\ldots,s_{rm})})$. Then the advantage of the distinguisher $\mathcal{A}$ is defined as

$$Adv_A(f, f^*) = \mid p_1 - p_0 \mid .$$

Assume that the distinguisher $\mathcal{A}$ is restricted to make at most q queries to the oracle $\mathcal{O}$, where q is some polynomial in n. We say that $\mathcal{A}$ is a pseudorandom distinguisher if it queries x and the oracle answers $y = \varphi(x)$, where φ is randomly chosen function by $\mathcal{O}$.

Definition 5 *A function $h : N \to R$ is negligible if for any constant $c > 0$ and all sufficiently large $n \in N$, $h(n) < \frac{1}{n^c}$.*

Definition 6 *Let $\boldsymbol{B}_n$ be an efficiently computable function ensemble. $\boldsymbol{B}_n$ is called a pseudorandom function ensemble if Adv_A is negligible for any pseudorandom distinguisher $\mathcal{A}$.*

In Definition 6, a function ensemble is efficiently computable if all functions in the ensemble can be computed efficiently. The following Theorem 1, which was first proved in [19], and equivalent versions of which can be found in [22], is a very useful tool for establishing upper bound on the Adv_A.

Theorem 1 *Let f be a random function of $\boldsymbol{F}_{n,n}$, f^* be a perfect random function of $\boldsymbol{F}_{n,n}$, q be an integer and $\mathcal{X}$ denote the $(\{0,1\}^n)^q$ set of all $x = (x_1, \ldots, x_q)$ q-tuples of pairwise distinct elements. If there exists a $\mathcal{Y}$ subset of $(\{0,1\}^n)^q$ and two positive real numbers ε_1 and ε_2 such that*

1) $|\mathcal{Y}| > 2^{qn}(1 - \varepsilon_1)$,

2) $\forall x \in \mathcal{X}, \forall y \in \mathcal{Y}, Pr[x \xrightarrow{f} y] \geq 2^{-qn}(1 - \varepsilon_2)$,

then for any distinguisher $\mathcal{A}$ using q queries

$$Adv_A(f, f^*) \leq \varepsilon_1 + \varepsilon_2.$$

3 Estimating the Security Against Differential/Linear Cryptanalysis

For simplification, let $m = 4$ in this section, denote as $GFSP_4$. We suppose all s-boxes $\{s_{11}, s_{12}, s_{13}, s_{14}, s_{21}, \ldots\}$ are permutations, so the round functions are also permutations. Let $(x_{4i+3}, x_{4i+2}, x_{4i+1}, x_{4i})$ and $(\triangle x_{4i+3}, \triangle x_{4i+2}, \triangle x_{4i+1}, \triangle x_{4i})$ denote the input and input difference of the $(i+1)th$ round. Here we don't consider the difference value, let "1" denote the non-zero difference. Hence, non-zero input difference only have fifteen denotations: $1 = (0001), \ldots, 15 = (1111)$.

3.1 Four Round $GFSP_4$

If input difference is "1", we have the following 4-round differential characteristics.

$$1 = (0001) \to (1001) \to (1101) \to \left\{ \begin{array}{lcl} (1111) & = & 15 \\ (1110) & = & 14. \end{array} \right.$$

Because the round function is permutation, the output difference is non-zero if the input difference is non-zero. Hence, the first 3-round differential characteristic is clear. For the fourth round, $F(\triangle x_{12})$ is likely to equal $\triangle x_{13}$ when $\triangle x_{12}$ and $\triangle x_{13}$ are non-zero. Hence, the output difference of the fourth round have two cases. The input difference of four round functions are all non-zero, which are $\triangle x_0, \triangle x_4, \triangle x_8$ and $\triangle x_{12}$. We denote the above 4-round differential characteristic as follows:

$$1 \left\{ \begin{array}{ll} \xrightarrow{4(4)} 14 & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{12} \\ \xrightarrow{4(4)} 15 & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{12} \end{array} \right.$$

Similarly, we have

$$2 \xrightarrow{4(3)} 15 \quad \triangle x_4 \triangle x_8 \triangle x_{12} \qquad\qquad 4 \xrightarrow{4(2)} 13 \quad \triangle x_8 \triangle x_{12}$$

$$3 \left\{ \begin{array}{ll} \xrightarrow{4(1)} 1 & \triangle x_0 \\ \xrightarrow{4(4)} 14 & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{12} \\ \xrightarrow{4(4)} 15 & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{12} \end{array} \right.$$

$$5 \left\{ \begin{array}{ll} \xrightarrow{4(2)} 3 & \triangle x_0 \triangle x_4 \\ \xrightarrow{4(4)} 14 & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{12} \\ \xrightarrow{4(4)} 15 & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{12} \end{array} \right.$$

$$6 \left\{ \begin{array}{ll} \xrightarrow{4(1)} 2 & \triangle x_4 \\ \xrightarrow{4(3)} 15 & \triangle x_4 \triangle x_8 \triangle x_{12} \end{array} \right. \qquad 8 \xrightarrow{4(1)} 9 \quad \triangle x_{12}$$

$$7 \left\{ \begin{array}{ll} \xrightarrow{4(2)} 3 & \triangle x_0 \triangle x_4 \\ \xrightarrow{4(3)} 12 & \triangle x_0 \triangle x_8 \triangle x_{12} \\ \xrightarrow{4(3)} 13 & \triangle x_0 \triangle x_8 \triangle x_{12} \\ \xrightarrow{4(4)} 14 & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{12} \\ \xrightarrow{4(4)} 15 & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{12} \end{array} \right.$$

$$9\begin{cases} \xrightarrow{4(3)} 7 & \triangle x_0\triangle x_4\triangle x_8 \\ \xrightarrow{4(4)} 14 & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12} \\ \xrightarrow{4(4)} 15 & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12} \end{cases}$$

$$10\begin{cases} \xrightarrow{4(2)} 6 & \triangle x_4\triangle x_8 \\ \xrightarrow{4(3)} 15 & \triangle x_4\triangle x_8\triangle x_{12} \end{cases} \quad 12\begin{cases} \xrightarrow{4(1)} 4 & \triangle x_8 \\ \xrightarrow{4(2)} 13 & \triangle x_8\triangle x_{12} \end{cases}$$

$$11\begin{cases} \xrightarrow{4(3)} 7 & \triangle x_0\triangle x_4\triangle x_8 \\ \xrightarrow{4(2)} 8 & \triangle x_0\triangle x_{12} \\ \xrightarrow{4(2)} 9 & \triangle x_0\triangle x_{12} \\ \xrightarrow{4(4)} 14 & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12} \\ \xrightarrow{4(4)} 15 & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12} \end{cases}$$

$$13\begin{cases} \xrightarrow{4(2)} 5 & \triangle x_0\triangle x_8 \\ \xrightarrow{4(3)} 12 & \triangle x_0\triangle x_8\triangle x_{12} \\ \xrightarrow{4(3)} 13 & \triangle x_0\triangle x_8\triangle x_{12} \end{cases}$$

$$14\begin{cases} \xrightarrow{4(2)} 6 & \triangle x_4\triangle x_8 \\ \xrightarrow{4(2)} 11 & \triangle x_4\triangle x_{12} \\ \xrightarrow{4(3)} 15 & \triangle x_4\triangle x_8\triangle x_{12} \end{cases}$$

$$15\begin{cases} \xrightarrow{4(2)} 5 & \triangle x_0\triangle x_8 \\ \xrightarrow{4(3)} 7 & \triangle x_0\triangle x_4\triangle x_8 \\ \xrightarrow{4(3)} 10 & \triangle x_0\triangle x_4\triangle x_{12} \\ \xrightarrow{4(3)} 11 & \triangle x_0\triangle x_4\triangle x_{12} \\ \xrightarrow{4(3)} 12 & \triangle x_0\triangle x_8\triangle x_{12} \\ \xrightarrow{4(3)} 13 & \triangle x_0\triangle x_8\triangle x_{12} \\ \xrightarrow{4(4)} 14 & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12} \\ \xrightarrow{4(4)} 15 & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12} \end{cases}$$

3.2 Eight Round $GFSP_4$

When the input difference is "1", the 8-round differential characteristics are the following:

$$1\begin{cases} \xrightarrow{4(4)} 14 \begin{cases} \xrightarrow{4(2)} 6, & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12}\triangle x_{20}\triangle x_{24} \\ \xrightarrow{4(2)} 11, & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12}\triangle x_{20}\triangle x_{28} \\ \xrightarrow{4(3)} 15, & \\ & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12}\triangle x_{20}\triangle x_{24}\triangle x_{28} \end{cases} \\ \xrightarrow{4(4)} 15 \begin{cases} \xrightarrow{4(2)} 5, & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12}\triangle x_{16}\triangle x_{24} \\ \xrightarrow{4(3)} 7, & \\ & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12}\triangle x_{16}\triangle x_{20}\triangle x_{24} \\ \xrightarrow{4(3)} 10(11), & \\ & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12}\triangle x_{16}\triangle x_{20}\triangle x_{24} \\ \xrightarrow{4(3)} 12(13), & \\ & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12}\triangle x_{16}\triangle x_{24}\triangle x_{28} \\ \xrightarrow{4(4)} 14(15), & \\ & \triangle x_0\triangle x_4\triangle x_8\triangle x_{12}\triangle x_{16}\triangle x_{20}\triangle x_{24}\triangle x_{28} \end{cases} \end{cases}$$

We show the minimum number of differential active s-boxes for 8-round $GFSP_4$ is equal or lager than $2P_d+1$, which is denoted as $N_1(S) \geq 2P_d+1$.

We first exemplify $1 \xrightarrow{4(4)} 14 \xrightarrow{4(2)} 6$.

When $\triangle y = \triangle x \oplus \triangle z$, we have $H_w(\triangle y) \leq H_w(\triangle x) + H_w(\triangle z)$. Let $\triangle y_i = F(x) \oplus F(x \oplus \triangle x_i)$. From the structure of 8-round $GFSP_4$, we have

$$\begin{array}{ll} \triangle y_0 = \triangle x_1 \oplus \triangle x_4, & \triangle y_4 = \triangle x_2 \oplus \triangle x_8, \\ \triangle y_8 = \triangle x_3 \oplus \triangle x_{12}, & \triangle y_{12} = \triangle x_0 \oplus \triangle x_{16}, \\ \triangle y_{16} = \triangle x_4 \oplus \triangle x_{20}, & \triangle y_{20} = \triangle x_8 \oplus \triangle x_{24}, \\ \triangle y_{24} = \triangle x_{12} \oplus \triangle x_{28}. & \end{array}$$

From the definition of branch number of P_d, we have

$$H_w(\triangle y_i) + H_w(\triangle x_i) \geq P_d.$$

Therefore, we have

$$\begin{array}{l} H_w(\triangle x_0) + H_w(\triangle x_1) + H_w(\triangle x_4) \geq P_d, \\ H_w(\triangle x_2) + H_w(\triangle x_4) + H_w(\triangle x_8) \geq P_d, \\ H_w(\triangle x_3) + H_w(\triangle x_8) + H_w(\triangle x_{12}) \geq P_d, \\ H_w(\triangle x_0) + H_w(\triangle x_{12}) + H_w(\triangle x_{16}) \geq P_d, \\ H_w(\triangle x_4) + H_w(\triangle x_{16}) + H_w(\triangle x_{20}) \geq P_d, \\ H_w(\triangle x_8) + H_w(\triangle x_{20}) + H_w(\triangle x_{24}) \geq P_d, \\ H_w(\triangle x_{12}) + H_w(\triangle x_{24}) + H_w(\triangle x_{28}) \geq P_d. \end{array}$$

For $1 \xrightarrow{4(4)} 14 \xrightarrow{4(2)} 6$, $H_w(\triangle x_1) = 0$,

$$\begin{array}{rcl} N_1(S) & = & H_w(\triangle x_0) + H_w(\triangle x_4) + H_w(\triangle x_8) \\ & + & H_w(\triangle x_{12}) + H_w(\triangle x_{20}) + H_w(\triangle x_{24}) \\ & = & [H_w(\triangle x_0) + H_w(\triangle x_1) + H_w(\triangle x_4)] \\ & + & [H_w(\triangle x_8) + H_w(\triangle x_{20}) + H_w(\triangle x_{24})] \\ & + & H_w(\triangle x_{12}) \\ & & \geq 2P_d + 1 \end{array}$$

Similarly, we can get $N_2(S) \geq 2P_d+1$, $N_3(S) \geq 2P_d+1$, $N_4(S) \geq 2P_d+1$, and $N_8(S) \geq 2P_d+1$. The other cases are as follows:

$$5\begin{cases} N_5(S) \geq P_d+1, & 5 \xrightarrow{4(2)} 3 \xrightarrow{4(1)} 1, \quad \triangle x_4\triangle x_8\triangle x_{16} \\ N_5(S) \geq 2P_d+1, & else \end{cases}$$

$$6\begin{cases} N_6(S) \geq P_d+2, & 6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15, \\ & \triangle x_4\triangle x_{20}\triangle x_{24}\triangle x_{28} \\ N_6(S) \geq 2P_d+1, & else \end{cases}$$

$$7\begin{cases} N_7(S) \geq P_d+1, & 7 \xrightarrow{4(2)} 3 \xrightarrow{4(1)} 1, \\ & \triangle x_0\triangle x_4\triangle x_{16} \\ N_7(S) \geq P_d+2, & 7 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4, \\ & \triangle x_0\triangle x_8\triangle x_{12}\triangle x_{24} \\ N_7(S) \geq P_d+3, & 7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13, \\ & \triangle x_0\triangle x_8\triangle x_{12}\triangle x_{24}\triangle x_{28} \\ N_6(S) \geq 2P_d+1, & else \end{cases}$$

$$9\begin{cases} N_9(S) \geq P_d+3, & 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3, \\ & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{16} \triangle x_{20} \\ N_6(S) \geq 2P_d+1, & else \end{cases}$$

$$10\begin{cases} N_{10}(S) \geq P_d+3, & 10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15, \\ & \triangle x_4 \triangle x_8 \triangle x_{20} \triangle x_{24} \triangle x_{28} \\ N_{10}(S) \geq P_d+1, & 10 \xrightarrow{4(2)} 6 \xrightarrow{4(1)} 2, \\ & \triangle x_4 \triangle x_8 \triangle x_{20} \\ N_6(S) \geq 2P_d+1, & else \end{cases}$$

$$11\begin{cases} N_{11}(S) \geq P_d+3, & 11 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3, \\ & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{16} \triangle x_{20} \\ N_{11}(S) \geq P_d+1, & 11 \xrightarrow{4(2)} 8 \xrightarrow{4(1)} 9, \\ & \triangle x_0 \triangle x_{12} \triangle x_{28} \\ N_6(S) \geq 2P_d+1, & else \end{cases}$$

$$12\begin{cases} N_{12}(S) \geq P_d+2, & 12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15, \\ & \triangle x_8 \triangle x_{20} \triangle x_{24} \triangle x_{28} \\ N_6(S) \geq 2P_d+1, & else \end{cases}$$

$$13\begin{cases} N_{13}(S) \geq P_d+2, & 13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3, \\ & \triangle x_0 \triangle x_8 \triangle x_{16} \triangle x_{20} \\ N_{13}(S) \geq P_d+2, & 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4, \\ & \triangle x_0 \triangle x_8 \triangle x_{12} \triangle x_{24} \\ N_{13}(S) \geq P_d+3, & 13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13, \\ & \triangle x_0 \triangle x_8 \triangle x_{12} \triangle x_{24} \triangle x_{28} \\ N_{13}(S) \geq 2P_d+1, & else \end{cases}$$

$$14\begin{cases} N_{13}(S) \geq P_d+3, & 14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15, \\ & \triangle x_4 \triangle x_8 \triangle x_{20} \triangle x_{24} \triangle x_{28} \\ N_{14}(S) \geq P_d+1, & 14 \xrightarrow{4(2)} 6 \xrightarrow{4(1)} 2, \\ & \triangle x_4 \triangle x_8 \triangle x_{20} \\ N_{14}(S) \geq P_d+2, & 14 \xrightarrow{4(2)} 11 \xrightarrow{4(2)} 8(9), \\ & \triangle x_4 \triangle x_{12} \triangle x_{16} \triangle x_{28} \\ N_{13}(S) \geq 2P_d+1, & else \end{cases}$$

$$15\begin{cases} N_{15}(S) \geq P_d+2, & 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3, \\ & \triangle x_0 \triangle x_8 \triangle x_{16} \triangle x_{20} \\ N_{15}(S) \geq P_d+2, & 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3, \\ & \triangle x_0 \triangle x_4 \triangle x_8 \triangle x_{16} \triangle x_{20} \\ N_{15}(S) \geq P_d+3, & 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8(9), \\ & \triangle x_0 \triangle x_4 \triangle x_{12} \triangle x_{16} \triangle x_{28} \\ N_{15}(S) \geq P_d+2, & 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4, \\ & \triangle x_0 \triangle x_8 \triangle x_{12} \triangle x_{24} \\ N_{15}(S) \geq P_d+3, & 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13, \\ & \triangle x_0 \triangle x_8 \triangle x_{12} \triangle x_{24} \triangle x_{28} \\ N_{15}(S) \geq 2P_d+1, & else \end{cases}$$

From the above discussion, we get the following Lemma.

Lemma 1 *If round functions are permutations, the minimum number of differential active s-boxes for 8-round $GFPN_4$ scheme is equal or larger than P_d+1.*

3.3 Sixteen Round $GFSP_4$

Theorem 2 *If round functions are permutations, the minimum number of differential active s-boxes for 16-round $GFPN_4$ scheme is equal or larger than $3P_d+1$.*

Proof. We first list the 8-round differentials which satisfy $N_i(S) < 2P_d+1$.

$$5 \xrightarrow{4(2)} 3 \xrightarrow{4(1)} 1,\ 6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15,\ 7 \xrightarrow{4(2)} 3 \xrightarrow{4(1)} 1,$$
$$7 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4,\ 7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,\ 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$10 \xrightarrow{4(2)} 6 \xrightarrow{4(1)} 2,\ 10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15,\ 11 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$11 \xrightarrow{4(2)} 8 \xrightarrow{4(1)} 9,\ 12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15,$$
$$13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,\ 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4,$$
$$13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,\ 14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15,$$
$$14 \xrightarrow{4(2)} 6 \xrightarrow{4(1)} 2,\ 14 \xrightarrow{4(2)} 11 \xrightarrow{4(2)} 8,$$
$$14 \xrightarrow{4(2)} 11 \xrightarrow{4(2)} 9,\ 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,\ 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8,\ 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9,$$
$$15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,\ 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4.$$

Since $N_1(S) \geq 2P_d+1$, $N_2(S) \geq 2P_d+1$, $N_3(S) \geq 2P_d+1$, $N_4(S) \geq 2P_d+1$, and $N_8(S) \geq 2P_d+1$, the 16-round differential of $GFSP_4$, whose number of active s-boxes is less than $3P_d+1$, must include in the following differentials.

$$11 \xrightarrow{4(2)} 8 \xrightarrow{4(1)} 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$14 \xrightarrow{4(2)} 11 \xrightarrow{4(2)} 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,$$
$$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8,$$
$$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9,$$
$$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,$$
$$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(1)} 4,$$
$$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,$$
$$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8,$$
$$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9,$$
$$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,$$
$$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4,$$
$$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,$$
$$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8,$$
$$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9,$$
$$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,$$

$$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4,$$
$$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,$$
$$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3,$$
$$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8,$$
$$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9,$$
$$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,$$
$$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(1)} 4,$$
$$7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,$$
$$7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4,$$
$$7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,$$
$$13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,$$
$$13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4,$$
$$13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13,$$
$$15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3,$$
$$15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4,$$
$$15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13.$$

From the structure of 16-round $GFSP_4$, we have

$$\begin{array}{ll}
\triangle y_0 = \triangle x_1 \oplus \triangle x_4, & \triangle y_4 = \triangle x_2 \oplus \triangle x_8, \\
\triangle y_8 = \triangle x_3 \oplus \triangle x_{12}, & \triangle y_{12} = \triangle x_0 \oplus \triangle x_{16}, \\
\triangle y_{16} = \triangle x_4 \oplus \triangle x_{20}, & \triangle y_{20} = \triangle x_8 \oplus \triangle x_{24}, \\
\triangle y_{24} = \triangle x_{12} \oplus \triangle x_{28}, & \triangle y_{28} = \triangle x_{16} \oplus \triangle x_{32}, \\
\triangle y_{32} = \triangle x_{20} \oplus \triangle x_{36}, & \triangle y_{36} = \triangle x_{24} \oplus \triangle x_{40}, \\
\triangle y_{40} = \triangle x_{28} \oplus \triangle x_{44}, & \triangle y_{44} = \triangle x_{32} \oplus \triangle x_{48}, \\
\triangle y_{48} = \triangle x_{36} \oplus \triangle x_{52}, & \triangle y_{52} = \triangle x_{40} \oplus \triangle x_{56}, \\
\triangle y_{56} = \triangle x_{44} \oplus \triangle x_{60}, & \triangle y_{60} = \triangle x_{48} \oplus \triangle x_{64}.
\end{array}$$

From the definition of branch number of P_d, If $\triangle x_i \neq 0$, then

$$H_w(\triangle y_i) + H_w(\triangle x_i) \geq P_d.$$

Therefore, we have

$$\begin{array}{ll}
If & \triangle x_0 \neq 0, \\
& then\ H_w(\triangle x_0) + H_w(\triangle x_1) + H_w(\triangle x_4) \geq P_d. \\
If & \triangle x_4 \neq 0, \\
& then\ H_w(\triangle x_2) + H_w(\triangle x_4) + H_w(\triangle x_8) \geq P_d. \\
If & \triangle x_8 \neq 0, \\
& then\ H_w(\triangle x_3) + H_w(\triangle x_8) + H_w(\triangle x_{12}) \geq P_d. \\
If & \triangle x_{12} \neq 0, \\
& then\ H_w(\triangle x_0) + H_w(\triangle x_{12}) + H_w(\triangle x_{16}) \geq P_d. \\
If & \triangle x_{16} \neq 0, \\
& then\ H_w(\triangle x_4) + H_w(\triangle x_{16}) + H_w(\triangle x_{20}) \geq P_d. \\
If & \triangle x_{20} \neq 0, \\
& then\ H_w(\triangle x_8) + H_w(\triangle x_{20}) + H_w(\triangle x_{24}) \geq P_d. \\
If & \triangle x_{24} \neq 0, \\
& then\ H_w(\triangle x_{12}) + H_w(\triangle x_{24}) + H_w(\triangle x_{28}) \geq P_d. \\
If & \triangle x_{28} \neq 0, \\
& then\ H_w(\triangle x_{16}) + H_w(\triangle x_{28}) + H_w(\triangle x_{32}) \geq P_d. \\
If & \triangle x_{32} \neq 0, \\
& then\ H_w(\triangle x_{20}) + H_w(\triangle x_{32}) + H_w(\triangle x_{36}) \geq P_d. \\
If & \triangle x_{36} \neq 0, \\
& then\ H_w(\triangle x_{24}) + H_w(\triangle x_{36}) + H_w(\triangle x_{40}) \geq P_d. \\
If & \triangle x_{40} \neq 0, \\
& then\ H_w(\triangle x_{28}) + H_w(\triangle x_{40}) + H_w(\triangle x_{44}) \geq P_d. \\
If & \triangle x_{44} \neq 0, \\
& then\ H_w(\triangle x_{32}) + H_w(\triangle x_{44}) + H_w(\triangle x_{48}) \geq P_d. \\
If & \triangle x_{48} \neq 0, \\
& then\ H_w(\triangle x_{36}) + H_w(\triangle x_{48}) + H_w(\triangle x_{52}) \geq P_d. \\
If & \triangle x_{52} \neq 0, \\
& then\ H_w(\triangle x_{40}) + H_w(\triangle x_{52}) + H_w(\triangle x_{56}) \geq P_d. \\
If & \triangle x_{56} \neq 0, \\
& then\ H_w(\triangle x_{44}) + H_w(\triangle x_{56}) + H_w(\triangle x_{60}) \geq P_d. \\
If & \triangle x_{60} \neq 0, \\
& then\ H_w(\triangle x_{48}) + H_w(\triangle x_{60}) + H_w(\triangle x_{64}) \geq P_d.
\end{array}$$

We exemplify $11 \xrightarrow{4(2)} 8 \xrightarrow{4(1)} 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$, whose non-zero inputs for round functions are $\triangle x_0 \triangle x_{12} \triangle x_{28} \triangle x_{32} \triangle x_{36} \triangle x_{40} \triangle x_{48} \triangle x_{52}$, and $\triangle x_4 = \triangle x_8 = \triangle x_{16} = \triangle x_{20} = \triangle x_{24} = \triangle x_{44} = \triangle x_{56} = \triangle x_{60} = 0$. Hence, the number of active boxes is

$$\begin{array}{l}
H_w(\triangle x_0) + H_w(\triangle x_{12}) + H_w(\triangle x_{28}) + H_w(\triangle x_{32}) \\
+H_w(\triangle x_{36}) + H_w(\triangle x_{40}) + H_w(\triangle x_{48}) + H_w(\triangle x_{52}) \\
= [H_w(\triangle x_0) + H_w(\triangle x_{12})] + H_w(\triangle x_{28}) \\
+[H_w(\triangle x_{32}) + H_w(\triangle x_{36})] + \\
[H_w(\triangle x_{40}) + H_w(\triangle x_{52})] + H_w(\triangle x_{48}) \\
\geq P_d + P_d + P_d + 2 = 3P_d + 2.
\end{array}$$

□

We can prove the other differentials similarly. There is a kind of "duality" relation between differential cryptanalysis and linear cryptanalysis. Hence, from Theorem 2 we have the following theorem.

Theorem 3 *Let p_S and q_S be the maximum differential/linear probabilities of all s-boxes$\{s_{11}, s_{12}, s_{13}, s_{14}, s_{21}, \ldots, s_{16,4}\}$. If the round functions are permutations, then the maximum differential/linear characteristic probabilities of 16-round $GFSP_4$ scheme are bounded by $(p_s)^{3P_d+1}$ and $(q_s)^{3P_d+1}$, respectively.*

4 7-Round Distinguishers

We discuss the pseudorandomness of n-bit r-round $GFSP$ scheme. $GFSP^{(f_{11}, f_{12}, \ldots, f_{rm})}$ hereafter, where $f_{ij} (i = 1, \ldots, r, j = 1, \ldots, m)$ are rm independent random functions from $\{0,1\}^l$ to $\{0,1\}^l$. We first present some 7-round distinguishers.

Choose

$$x_3 = (x, a_{3,2}, \cdots, a_{3,m}), \quad x_2 = (a_{2,1}, a_{2,2}, \cdots, a_{2,m}),$$
$$x_1 = (a_{1,1}, a_{1,2}, \cdots, a_{1,m}), \quad x_0 = (a_{0,1}, a_{0,2}, \cdots, a_{0,m}).$$

where x take values in $\{0,1\}^l$, $a_{i,j}$ are constants in $\{0,1\}^l$. Thus the input of the $4th$ round can be written as follows:

$$\begin{aligned} x_{15} &= (a_{15,1}, a_{15,2}, \cdots, a_{15,m}),\\ x_{14} &= (a_{14,1}, a_{14,2}, \cdots, a_{14,m}),\\ x_{13} &= (a_{13,1}, a_{13,2}, \cdots, a_{13,m}),\\ x_{12} &= (x \oplus a_{12,1}, a_{12,2}, \cdots, a_{12,m}). \end{aligned}$$

where $a_{i,j}(12 \le i \le 15, 1 \le j \le m)$ are entirely determined by $a_{i,j}(0 \le i \le 3, 1 \le j \le m)$ and functions $f_{i,j}(1 \le i \le 3, 1 \le j \le m)$, so $a_{i,j}(12 \le i \le 15, 1 \le j \le m)$ are constants when $f_{i,j}(1 \le i \le 3, 1 \le j \le m)$ are fixed.

In the $4th$ round a transformation on $x_{12} = (x \oplus a_{12,1}, a_{12,2}, \cdots, a_{12,m})$ using F_4 is as follows: $x_{12} = (x \oplus a_{12,1}, a_{12,2}, \cdots, a_{12,m}) \xrightarrow{F_4} (\theta_{11}y \oplus b_1, \theta_{11}y \oplus b_2, \ldots, \theta_{11}y \oplus b_m)$, where $y = f_{41}(x \oplus a_{12,1})$, $b_j(1 \le j \le m)$ are entirely determined by $a_{12,j}(2 \le j \le m)$ and $f_{4j}(2 \le j \le m)$, thus $b_j(1 \le j \le m)$ are constants when $f_{4j}(2 \le j \le m)$ are fixed. Therefore, the input of the $5th$ round is

$$\begin{aligned} x_{19} &= x_{12},\\ x_{18} &= x_{15},\\ x_{17} &= x_{14},\\ x_{16} &= x_{13} \oplus F_4(x_{12})\\ &= (\theta_{11}y \oplus b_1 \oplus a_{13,1}, \ldots, \theta_{11}y \oplus b_m \oplus a_{13,m}). \end{aligned}$$

The one block of output for 7th round is as follows:

$$x_{29} = x_{16} = (\theta_{11}y \oplus b_1 \oplus a_{13,1}, \ldots, \theta_{11}y \oplus b_m \oplus a_{13,m})$$

So we get $x_{29,1} \oplus x_{29,2} = b_1 \oplus a_{13,1} \oplus b_2 \oplus a_{13,m}$ is a constant. Similarly we have the following lemma:

Lemma 2 *Let $P = (x_3, x_2, x_1, x_0)$ and $P^* = (x_3^*, x_2^*, x_1^*, x_0^*)$ be two plaintexts of 7-round GFSP, $C = (x_{31}, x_{30}, x_{29}, x_{28})$ and $C^* = (x_{31}^*, x_{30}^*, x_{29}^*, x_{28}^*)$ be corresponding ciphertexts, $x_{0,i}$ denote the $i-th$ sub-block of x_0. If $x_0 = x_0^*, x_1 = x_1^*, x_2 = x_2^*$, $x_{3,1} \neq x_{3,1}^*$, $x_{3,j} = x_{3,j}^*(2 \le j \le m)$, then for any subset $I \subseteq \{1, 2, \ldots, m\}$, if $|I|$ is even, then*

$$\bigoplus_{j \in I} x_{29,j} = \bigoplus_{j \in I} x_{29,j}^*$$

5 Pseudorandomness of $GFSP$

5.1 7-Round $GFSP$ Is Not A Pseudorandom Function

Theorem 4 *Let $f_{11}, \ldots, f_{1m}, f_{21}, \ldots, f_{7m}$ be $7m$ independent random functions from $\{0,1\}^l$ to $\{0,1\}^l$ and f^* be the perfect random function on $\{0,1\}^n$ and $f = GFSP^{(f_{11}, f_{12}, \ldots, f_{7m})}$. There exists a non-adaptive distinguisher $\mathcal{A}$ with q queries such that:*

$$Adv_A \ge 1 - 2^{-\frac{n(m-1)}{8}} \quad .$$

Proof. We consider a distinguisher $\mathcal{A}$ as follows.

1) $\mathcal{A}$ randomly chooses two plaintexts $P = (x_3, x_2, x_1, x_0)$ and $P^* = (x_3^*, x_2^*, x_1^*, x_0^*)$ such that $x_0 = x_0^*, x_1 = x_1^*, x_2 = x_2^*$, $x_{3,1} \neq x_{3,1}^*$, $x_{3,j} = x_{3,j}^*(2 \le j \le m)$.

2) $\mathcal{A}$ sends them to the oracle and receives the ciphertexts $C = (x_{31}, x_{30}, x_{29}, x_{28})$ and $C^* = (x_{31}^*, x_{30}^*, x_{29}^*, x_{28}^*)$ from the oracle.

3) Finally, $\mathcal{A}$ outputs 1 if and only if for any $1 \le j_1 < j_2 \le m$,

$$x_{29,j_1} \oplus x_{29,j_2} = x_{29,j_1}^* \oplus x_{29,j_2}^*$$

Suppose that the oracle implements f^*, then it is clear that $p_0 = 2^{-\frac{n(m-1)}{8}}$. Next suppose that the oracle implements $f = GFSP^{(f_{11}^*, f_{12}^*, \ldots, f_{7m}^*)}$. Using Lemma 2, we get $p_1 = 1$. Therefore, we obtained that

$$Adv_A(f, f^*) \ge 1 - 2^{-\frac{n(m-1)}{8}}$$

which is non-negligible. Hence, 7-round $GFSP$ is not a pseudorandom function.

□

5.2 8-Round $GFSP$ Is A Pseudorandom Function

Theorem 5 *Let $f_{11}^*, \ldots, f_{1m}^*, f_{21}^*, \ldots, f_{8m}^*$ be $8m$ independent random functions from $\{0,1\}^l$ to $\{0,1\}^l$ and f^* be the perfect random function on $\{0,1\}^n$ and $f = GFSP^{(f_{11}^*, f_{12}^*, \ldots, f_{8m}^*)}$. If the branch number of linear transformation $P : (\{0,1\}^l)^m \to (\{0,1\}^l)^m$ is $m+1$, then for any adaptive distinguisher $\mathcal{A}$ with q queries we have*

$$Adv_A(f, f^*) \le 13q^2 2^{-\frac{n}{4}}.$$

Proof. Let us first introduce some notation. We consider a $X = (X^1, X^2, \ldots, X^q) = (x_3^i, x_2^i, x_1^i, x_0^i)_{i \in [1,\ldots,q]}$ q-tuple of n-bit f input words. We denote the corresponding q-tuple of f output words by $Z = (z_{35}^i, x_{34}^i, x_{33}^i, x_{32}^i)_{i \in [1,\ldots,q]}$.

We denote the $(x_k^i)_{i \in [1,\ldots,q]}$ and $(y_k^i)_{i \in [1,\ldots,q]}$ q-tuples of $\frac{n}{4}$-bit words by $x_k^{[1 \sim q]}$ and $y_k^{[1 \sim q]}$. Let $(x_{4i+3}, x_{4i+2}, x_{4i+1}, x_{4i})$ be the input of $(i+1)th$ round and the output of ith round, and $x_j = (x_{j,1}, \ldots, x_{j,m})$. Let $I_n^{\neq}$ denotes the subset of $(\{0,1\}^n)^q$ consisting of all the q-tuples of pairwise distinct $\{0,1\}^n$ values.

We now define $\mathcal{X} = I_n^{\neq}$, $\mathcal{Y} = (Y^1, \ldots, Y^q) = \{(y_3^i, y_2^i, y_1^i, y_0^i)_{i \in [1,\ldots,q]} \mid (y_3^{[1 \sim q]} \in I_{\frac{n}{4}}^{\neq}) \wedge (y_2^{[1 \sim q]} \in I_{\frac{n}{4}}^{\neq}) \wedge (y_1^{[1 \sim q]} \in I_{\frac{n}{4}}^{\neq}) \wedge (y_0^{[1 \sim q]} \in I_{\frac{n}{4}}^{\neq})\}$. We want to establish a lower bound on the size of $\mathcal{Y}$ and the $Pr[X \to Y]$ for any X q-tuple in $\mathcal{X}$ and Y q-tuple in $\mathcal{Y}$ and show that there exists ε_1 and ε_2 real numbers satisfying conditions of Theorem 1.

Let us first establish a lower bound on $|\mathcal{Y}|$. We have:

$$\begin{aligned} |\mathcal{Y}| &\geq 2^{qn}(1 - Pr[(y_3^{[1\sim q]} \notin I^{\neq}_{\frac{n}{4}}) \vee (y_2^{[1\sim q]} \notin I^{\neq}_{\frac{n}{4}}) \\ &\quad \vee (y_1^{[1\sim q]} \notin I^{\neq}_{\frac{n}{4}}) \vee (y_0^{[1\sim q]} \notin I^{\neq}_{\frac{n}{4}})]) \\ &\geq 2^{qn}[1 - \sum_{1\leq i<j\leq q} Pr(y_3^i = y_3^j) \\ &\quad - \cdots - \sum_{1\leq i<j\leq q} Pr(y_0^i = y_0^j)] \\ &\geq 2^{qn}[1 - 2q(q-1)2^{-\frac{n}{4}}] \end{aligned}$$

So $\varepsilon_1 = 2q(q-1)2^{-\frac{n}{4}}$.

Now, given any X q-tuple in $\mathcal{X}$ and any Y q-tuple in $\mathcal{Y}$, let us establish a lower bound on $Pr[X \to Y]$.

$Pr[X \to Y] = Pr[Y^i = (y_3^i, y_2^i, y_1^i, y_0^i) = (x_{35}^i, x_{34}^i, x_{33}^i, x_{32}^i), i = 1, \ldots, q]$

$Y^i = (x_{35}^i, x_{34}^i, x_{33}^i, x_{32}^i)$ if and only if

$$\begin{aligned} y_0^i &= x_{32}^i = x_{29}^i \oplus F_8(x_{28}^i), \\ y_1^i &= x_{20}^i = x_{17}^i \oplus F_5(x_{16}^i), \\ y_2^i &= x_{24}^i = x_{21}^i \oplus F_6(x_{20}^i), \\ y_3^i &= x_{28}^i = x_{25}^i \oplus F_7(x_{24}^i). \end{aligned}$$

Let A^i be the event $[Y^i = (x_{35}^i, x_{34}^i, x_{33}^i, x_{32}^i)]$, $A = A^1 \wedge A^2 \wedge \cdots \wedge A^q$. Let B_{16}, B_{20}, B_{24} and B_{28} be the event $[x_{16}^{[1\sim q]} \in I^{\neq}_{\frac{n}{4}}], [x_{20}^{[1\sim q]} \in I^{\neq}_{\frac{n}{4}}], [x_{24}^{[1\sim q]} \in I^{\neq}_{\frac{n}{4}}]$ and $[x_{28}^{[1\sim q]} \in I^{\neq}_{\frac{n}{4}}]$, respectively. Let $B = B_{16} \wedge B_{20} \wedge B_{24} \wedge B_{28}$.

$Pr[X \to Y] = Pr[Y^i = (y_3^i, y_2^i, y_1^i, y_0^i) = (x_{35}^i, x_{34}^i, x_{33}^i, x_{32}^i), i = 1, \ldots, q]$
$= Pr[A] \geq Pr[A|B]Pr[B]$

Because $f_{51}, \ldots, f_{8m}$ are independent random functions, we have $Pr[A|B] = (2^{-n})^q$.

$$\begin{aligned} &Pr[B] = 1 - Pr[\overline{B_{16}} \vee \overline{B_{20}} \vee \overline{B_{24}} \vee \overline{B_{28}}] \\ &\geq 1 - [Pr(\overline{B_{16}}) + Pr(\overline{B_{20}}) + Pr(\overline{B_{24}}) + Pr(\overline{B_{28}})] \\ &\geq 1 - [\sum_{i\neq j} Pr(x_{16}^i = x_{16}^j) + \sum_{i\neq j} Pr(x_{20}^i = x_{20}^j) \\ &\quad + \sum_{i\neq j} Pr(x_{24}^i = x_{24}^j) + \sum_{i\neq j} Pr(x_{28}^i = x_{28}^j)] \end{aligned}$$

Next, we estimate $Pr(x_{16}^i = x_{16}^j), Pr(x_{20}^i = x_{20}^j), Pr(x_{24}^i = x_{24}^j)$ and $Pr(x_{28}^i = x_{28}^j)$.

$$\begin{aligned} &Pr(x_{16}^i = x_{16}^j) \\ &= Pr(x_{16}^i = x_{16}^j | x_{12}^i \neq x_{12}^j) Pr(x_{12}^i \neq x_{12}^j) \\ &\quad + Pr(x_{16}^i = x_{16}^j | x_{12}^i = x_{12}^j) Pr(x_{12}^i = x_{12}^j) \\ &\leq Pr(x_{16}^i = x_{16}^j | x_{12}^i \neq x_{12}^j) + Pr(x_{12}^i = x_{12}^j) \end{aligned}$$

Let us now estimate $Pr(x_{12}^i = x_{12}^j)$.

Case 1: If $(x_2^i, x_1^i, x_0^i) = (x_2^j, x_1^j, x_0^j)$, then $x_3^i \neq x_3^j$, so that $Pr(x_{12}^i = x_{12}^j) = 0$.

Case 2: If $(x_2^i, x_1^i, x_0^i) \neq (x_2^j, x_1^j, x_0^j)$

$$\begin{aligned} &Pr(x_{12}^i = x_{12}^j) \\ &= Pr(x_{12}^i = x_{12}^j | x_8^i \neq x_8^j) Pr(x_8^i \neq x_8^j) \\ &\quad + Pr(x_{12}^i = x_{12}^j | x_8^i = x_8^j) Pr(x_8^i = x_8^j) \\ &\leq Pr(x_{12}^i = x_{12}^j | x_8^i \neq x_8^j) + Pr(x_8^i = x_8^j) \end{aligned}$$

From $x_{12}^i = x_9^i \oplus F_3(x_8^i)$, the SP network of round function and $f_{31}, f_{32}, \ldots, f_{3m}$ are random functions, we have

$$Pr(x_{12}^i = x_{12}^j | x_8^i \neq x_8^j) \leq (2^{-l})^m = 2^{-\frac{n}{4}}$$

Further, estimate $Pr(x_8^i = x_8^j)$.

Case 2.1: If $(x_1^i, x_0^i) = (x_1^j, x_0^j)$, then $x_2^i \neq x_2^j$, so that $Pr(x_8^i = x_8^j) = 0$.

Case 2.2: If $(x_1^i, x_0^i) \neq (x_1^j, x_0^j)$, then $Pr(x_4^i = x_4^j) = \begin{cases} 0 & x_0^i = x_0^j \\ 2^{-\frac{n}{4}} & x_0^i \neq x_0^j \end{cases}$

$$\begin{aligned} &Pr(x_8^i = x_8^j) \\ &= Pr(x_8^i = x_8^j | x_4^i \neq x_4^j) Pr(x_4^i \neq x_4^j) \\ &\quad + Pr(x_8^i = x_8^j | x_4^i = x_4^j) Pr(x_4^i = x_4^j) \\ &\leq Pr(x_8^i = x_8^j | x_4^i \neq x_4^j) + Pr(x_4^i = x_4^j). \end{aligned}$$

From $x_8^i = x_5^i \oplus F_2(x_4^i)$, the SP network of round function and $f_{21}, f_{22}, \ldots, f_{2m}$ are random functions, we have

$$Pr(x_8^i = x_8^j | x_4^i \neq x_4^j) \leq (2^l)^m = 2^{-\frac{n}{4}}$$

In all cases, $Pr(x_8^i = x_8^j) \leq 2 \times 2^{-\frac{n}{4}}$, Hence we obtain

$$Pr(x_{12}^i = x_{12}^j) \leq 3 \times 2^{-\frac{n}{4}}.$$

Thus

$$\begin{aligned} &Pr(x_{16}^i = x_{16}^j) \\ &\leq Pr(x_{16}^i = x_{16}^j | x_{12}^i \neq x_{12}^j) + Pr(x_{12}^i = x_{12}^j) \\ &\leq 2^{-\frac{n}{4}} + 3 \times 2^{-\frac{n}{4}} = 4 \times 2^{-\frac{n}{4}}. \end{aligned}$$

Similarly, we have

$$\begin{aligned} &Pr(x_{20}^i = x_{20}^j) \leq 2^{-\frac{n}{4}} + 4 \times 2^{-\frac{n}{4}} = 5 \times 2^{-\frac{n}{4}}, \\ &Pr(x_{24}^i = x_{24}^j) \leq 2^{-\frac{n}{4}} + 5 \times 2^{-\frac{n}{4}} = 6 \times 2^{-\frac{n}{4}}, \\ &Pr(x_{28}^i = x_{28}^j) \leq 2^{-\frac{n}{4}} + 6 \times 2^{-\frac{n}{4}} = 7 \times 2^{-\frac{n}{4}}. \end{aligned}$$

Thus

$$Pr[B] \geq 1 - \frac{q(q-1)}{2} \times 22 \times 2^{-\frac{n}{4}}.$$

Hence, we have

$$Pr[X \xrightarrow{f} Y] \geq (2^{-\frac{n}{4}})^q [1 - 11q(q-1)2^{-\frac{n}{4}}].$$

We can notice that $Pr[X \xrightarrow{f^*} Y] = (2^{-n})^q$, so we can apply Theorem 1 with $\varepsilon_1 = 2q(q-1)2^{-\frac{n}{4}}$ and $\varepsilon_2 = 11q(q-1)2^{-\frac{n}{4}}$. We have

$$Adv_A(f, f^*) \leq \varepsilon_1 + \varepsilon_2 \leq 13q^2 2^{-\frac{n}{4}}.$$

This shows that the eight rounds $GFSP$ is a pseudorandom function for any adaptive adversaries. □

6 Concluding Remarks

Evaluating the security of block cipher mostly includes two aspects, the one is to evaluate the strength against differential/linear cryptanalysis and other attacks, the other is to study the pseudorandomness of the cipher scheme. In this paper we study the strength against differential/linear cryptanalysis and pseudorandomness of a generalized Feistel scheme with SP round function called $GFSP$. We focus on the minimum number of active s-boxes in some consecutive rounds of $GFSP_4$, i.e., in four, eight and sixteen consecutive rounds, since we can determine the upper bounds of the maximum differential/linear probabilities using the branch number of linear transformation P. As a result, we give the upper bounds of the maximum differential/linear probabilities of 16-round $GFSP_4$ scheme. Furthermore, we study the pseudorandomness of $GFSP$. We first present some distinguishers of seven rounds $GFSP$, then point out seven rounds $GFSP$ is not pseudorandom for non-adaptive adversary. Finally, we prove eight rounds $GFSP$ is pseudorandom for any adversaries.

Acknowledgment

We thank the anonymous referees for their helpful comments. This research is supported by the National Natural Science Foundation of China under Grant No.60373047; the National Basic Research 973 Program of China under Grant No.2004CB318004; the National High-Technology Development 863 Program of China under Grant No. 2003AA144030.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3-72, 1991.

[2] F. Chabaud, S. Vaudenay, "Links between differential and linear cryptanalysis," in *EUROCRYPT'94*, LNCS 950, pp. 356-365, Springer-Verlag, 1995.

[3] H. Gilbert and M.Minier, "New results on the pseudorandomness of some blockcipher constructions," *Fast Software Encryption - FSE2001*, LNCS 2355, pp. 248-266, Springer-Verlag, 2001.

[4] T. Iwata and K. Kurosawa, "On the pseudorandomness of the AES Finalists - RC6 and serpent," in *Fast Software Encryption - FSE2000*, LNCS 1978, pp. 231-243, Springer-Verlag, 2000.

[5] T. Iwata and K. Kurosawa, "On the correctness of security proofs for the 3GPP confidentiality and integrity algorithms," in *Cryptography and Coding 2003*, LNCS 2898, pp. 306-318, Springer-Verlag, 2003.

[6] T. Iwata, T. Yoshino, T. Yuasa and K. Kurosawa,"Round security and super-pseudorandomness of MISTY type structure", in *Fast Software Encryption - FSE2001*, LNCS 2355, pp. 233-247, Springer-Verlag, 2001.

[7] M. Kanda, "Practical security evaluation against differential and linear attacks for feistel ciphers with SPN round function," in *Selected Areas in Cryptography - SAC 2000*, LNCS 2012, pp. 168-179, Springer-Verlag, 2000.

[8] J. S. Kang, S. U. Shin, D. Hong, and O. Yi, "Provable security of KASUMI and 3GPP encryption mode F8," in *ASIACRYPT2001*, LNCS 2248, pp. 255-271, Springer-Verlag, 2001.

[9] L. R. Knudsen, "Practically secure Feistel ciphers", in *Fast Software Encryption - FSE'94*, pp. 211-221, Springer-Verlag, 1994.

[10] L. R. Knudsen, "The security of feistel ciphers with six rounds or less," *Journal of Cryptology*, vol. 15, no. 3, pp. 207-222, 2002.

[11] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 373-386, 1988.

[12] S. Lucks, "Faster Luby-Rackoff ciphers," in *Fast Software Encryption - FSE'96*, LNCS 1039, pp. 189-203, Springer-Verlag, 1996.

[13] M. Matsui, "Linear cryptanalysis method for DES cipher," in *EUROCRYPT'93*, LNCS 765, pp. 386-397, Springer-Verlag, 1994.

[14] U. M. Maurer, "A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators," in *EUROCRYPT'92*, LNCS 658, pp. 239-255, Springer-Verlag, 1992.

[15] S. Moriai and S. Vaudenay, "On the pseudorandomness of top-level schemes of block ciphers", in *ASIACRYPT 2000*, LNCS 1876, pp. 289-302, Springer-Verlag, 2000.

[16] M. Naor and O. Reingold, "On the construction of pseudorandom permutations Luby-Rackoff revisited," *Journal of Cryptology*, vol. 12, no. 1, pp. 29-66, 1999.

[17] K. Nyberg, "Perfect nonlinear S-boxes," in *EUROCRYPT'91*, LNCS 547, pp. 378-385, Springer-Verlag, 1991.

[18] K. Nyberg, L. R. Knudsen, "Provable security against a differential attack," *Journal of Cryptology*, vol. 8, no. 1, pp. 27-37, 1995.

[19] J. Patarin, "How to construct pseudorandom permutations from a single pseudorandom function", in *EUROCRYPT'92*, LNCS 658, pp. 256-266, Springer-Verlag, 1992.

[20] S. Patel, Z. Ramzan, and G. Sundaram, "Towards making Luby-Rackoff ciphers optimal and practical," in *Fast Software Encryption - FSE'99*, LNCS 1636, pp.171-185, Springer-Verlag, 1999.

[21] Z. Ramzan and L. Reyzin, "On the round security of symmetric-key cryptographic primitives," in *CRYPTO 2000*, LNCS 1880, pp.376-393, Springer-Verlag, 2000.

[22] S. Vaudenay, "On provable security of conventional cryptography," in *Information Security and Cryptography- ICISC'99*, LNCS 1787, pp. 1-16, Springer-Verlag,1999.

[23] Y. Zheng, T. Matsumoto, and H. Imai, "On the construction of block ciphers provably secure and not relying on any unproved hypotheses," in *CRYPTO'89*, LNCS 435, pp.461-480, Springer-Verlag, 1989.

Wenling Wu is now a professor at the State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences. She received her B.S. degree and M.S. degree in Maths from Northwest University in 1987 and 1990, respectively. She received her Ph.D degree in Cryptography from Xidian University in 1997. From 1998 to 1999 she was a postdoctoral fellow in the Institute of Software, Chinese Academy of Science. Her current research interests include theory of cryptography, mode of operation, block cipher, stream cipher and hash function.

Wentao Zhang is now an assistant professor at the State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences. She received her M.S. degree in Maths from Northwest University in 2000. She received her Ph.D degree in Computer science and technology from Institute of Software, Chinese Academy of Sciences in 2003. Her current research interest is the design and analysis of block cipher.

Dongdai Lin is now a full time research professor and deputy director of State Key Labortory of Information Security, Institute of Software of the Chinese Academy of Sciences. He received his B.S. degree in mathematics from Shandong University in 1984, and the M.S. degree and Ph. D degree in coding theory and cryptology at Institute of Systems Science of the Chinese Academy of Sciences in 1987 and 1990 respectively. His current research interests include cryptology, information security, grid computing, mathematics mechanization and symbolic computations.