

Security on Generalized Feistel Scheme with SP Round Function¹

Wu Wenling Zhang Wentao Lin Dongdai

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

Abstract. This paper studies the security against differential/linear cryptanalysis and the pseudorandomness for a class of generalized Feistel scheme with SP round function called *GFSP*. We consider 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, in order to evaluate the strength against differential/linear cryptanalysis. Furthermore, We investigate the pseudorandomness of *GFSP*, point out 7-round *GFSP* is not pseudorandom for non-adaptive adversary, by using some distinguishers, and prove that 8-round *GFSP* is pseudorandom for any adversaries.

Key words: Differential cryptanalysis, Linear cryptanalysis, Branch number, Cipher, S-box, Pseudorandomness.

1 Introduction

The well-known approaches to attacking block cipher are differential cryptanalysis, proposed by Biham and Shamir[1], and linear cryptanalysis, introduced by Matsui[2]. Nyberg[3,4] first formalizes the notion of strength against differential cryptanalysis. Similarly, Chabaud and Vaudenay[5] formalize 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[6] give the upper bounds of differential /linear characteristic probabilities for Feistel scheme, by using the minimum numbers of differential/linear active s-boxes. Kanda[7] shows the minimum numbers of differential/linear active s-boxes for Feistel scheme with SP round function. Another approach in order to study the security of block ciphers was introduced by Luby and Rackoff [8] 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 pseudorandomness and four round

¹ This work was supported by Chinese Natural Science Foundation (Grant No.60373047) and 973 Project (Grant No. 2004CB318004)

Feistel scheme is super-pseudorandomness. Maurer gave a simpler proof for non-adaptive adversaries[9]. Since then, many researchers tried to improve the results and prove the pseudorandomness of other schemes(see, for instance,[10~23]). Among these papers,[10] and [22] have shown 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 pseudorandomness. In their research work, they just suppose 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, and the linear transformation *P* in the round function is fixed and s-boxes are random functions. It is not known whether seven round *GFSP* scheme is pseudorandomness, and how many round *GFSP* scheme is pseudorandomness. We solve this problem, and show 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 7-round 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 Fig.1 and Fig.2). Note that we neglect the effect of the round key hereafter. *S*-function is a non-linear transformation layer with *m* parallel *l*-bit s-boxes. That is ,

$$S_i : (\{0, 1\}^l)^m \longrightarrow (\{0, 1\}^l)^m$$

$$x_j = (x_{j,1}, \dots, x_{j,m}) \longrightarrow z_j = S_i(x_j) = (s_{i1}(x_{j,1}), \dots, s_{im}(x_{j,m})).$$

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

$$P : (\{0, 1\}^l)^m \longrightarrow (\{0, 1\}^l)^m$$

$$z_j = (z_{j,1}, \dots, z_{j,m}) \longrightarrow y_j = P(z_j) = (y_{j,1}, \dots, y_{j,m}).$$

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

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

Finally, the i th round function can be described as follows:

$$F_i : (\{0, 1\}^l)^m \longrightarrow (\{0, 1\}^l)^m$$

$$x_j = (x_{j,1}, \dots, x_{j,m}) \longrightarrow y_j = PS_i(x_j) = P(z_j) = (y_{j,1}, \dots, y_{j,m}).$$

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:

$$x_{4i+4} = F_i(x_{4i}) \oplus x_{4i+1},$$

$$x_{4i+5} = x_{4i+2}.$$

$$x_{4i+6} = x_{4i+3},$$

$$x_{4i+7} = x_{4i+1}.$$

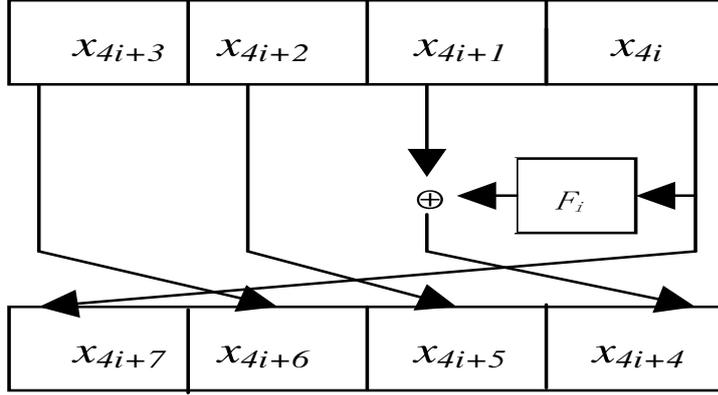


Fig. 1. The i -th round transformation

2.2 Definitions

We use the following definitions in this paper.

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

$$DP^s(\Delta x \rightarrow \Delta z) = \frac{|\{x \in \{0, 1\}^l | s(x) \oplus s(x \oplus \Delta x) = \Delta z\}|}{2^l}$$

$$LP^s(\Gamma z \rightarrow \Gamma x) = (2 \times \frac{|\{x \in \{0, 1\}^l | x \cdot \Gamma x = s(x) \cdot \Gamma z\}|}{2^l})_2$$

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

$$p_s = \max_{ij} \max_{\Delta x \neq 0, \Delta z} DP^{s_{ij}}(\Delta x \rightarrow \Delta z)$$

$$q_s = \max_{ij} \max_{\Gamma x, \Gamma z \neq 0} LP^{s_{ij}}(\Gamma z \rightarrow \Gamma x)$$

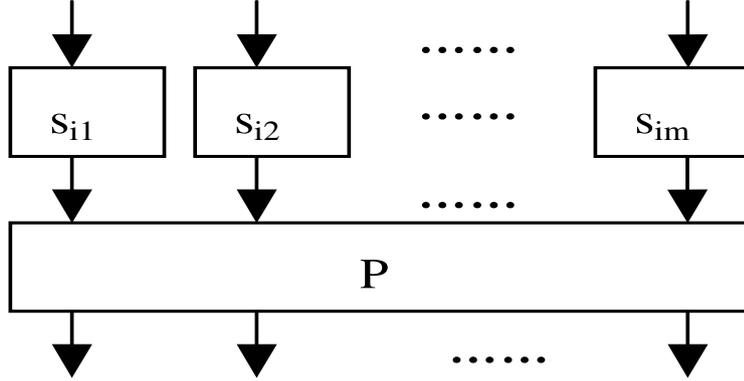


Fig. 2. The i -th round function F_i

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 $x_i = (x_{i1}, \dots, x_{im}) \in (\{0, 1\}^l)^m$, 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 $P : (\{0, 1\}^l)^m \rightarrow (\{0, 1\}^l)^m$ 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 $GFSP^{(s_{11}, s_{12}, \dots, s_{rm})}$ can be regarded as a random function of $\mathbf{F}_{n,n}$ determined by rm random functions $s_{ij} \in \mathbf{F}_{l,l}, i = 1, \dots, r, j = 1, \dots, m$. 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 $f = GFSP^{(s_{11}, s_{12}, \dots, s_{rm})}$ 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 $GFSP^{(s_{11}, s_{12}, \dots, s_{rm})}$ or $\mathbf{F}_{n,n}$. The aim of the distinguisher \mathcal{A} is to distinguish if the oracle \mathcal{O} implements $GFSP^{(s_{11}, s_{12}, \dots, s_{rm})}$ 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 $GFSP^{(s_{11}, s_{12}, \dots, s_{rm})}$. That is $p_0 = Pr(\mathcal{A} \text{ outputs } 1 \mid \mathcal{O} \leftarrow \mathbf{F}_{n,n})$ and $p_1 = Pr(\mathcal{A} \text{ outputs } 1 \mid \mathcal{O} \leftarrow GFSP^{(s_{11}, s_{12}, \dots, s_{rm})})$. Then the advantage of the distinguisher \mathcal{A} is defined as

$$Adv_{\mathcal{A}}(f, f^*) = |p_1 - p_0|$$

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

Definition 6. Let \mathbf{B}_n be an efficiently computable function ensemble. \mathbf{B}_n is called a pseudorandom function ensemble if $Adv_{\mathcal{A}}$ 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 [11], and equivalent versions of which can be found in [23], is a very useful tool for establishing upper bound on the $Adv_{\mathcal{A}}$.

Theorem 1. Let f be a random function of $\mathbf{F}_{n,n}$ and f^* a perfect random function of $\mathbf{F}_{n,n}$. Let q be an integer. Denote by \mathcal{X} the $(\{0, 1\}^n)^q$ set of all $x = (x_1, \dots, x_q)$ 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

$$Adv_{\mathcal{A}}(f, f^*) \leq \varepsilon_1 + \varepsilon_2$$

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 $\{s_{11}, s_{12}, s_{13}, s_{14}, s_{21}, \dots\}$ are permutations, so the round functions are also permutations. Let $(x_{4i+3}, x_{4i+2}, x_{4i+1}, x_{4i})$ and $(\Delta x_{4i+3}, \Delta x_{4i+2}, \Delta x_{4i+1}, \Delta x_{4i})$ 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: $1 = (0001), \dots, 15 = (1111)$.

3.1 Four Round $GFSP_4$

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

$$1 = (0001) \rightarrow (1001) \rightarrow (1101) \rightarrow \begin{cases} (1111) = 15 \\ (1110) = 14 \end{cases}$$

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, $F(\Delta x_{12})$ is likely to equal Δx_{13} when Δx_{12} and Δx_{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 $\Delta x_0, \Delta x_4, \Delta x_8$ and Δx_{12} . We denote the above 4-round differential characteristic as follows:

$$1 \begin{cases} \xrightarrow{4(4)} 14 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases}$$

Similarly, we have

$$\begin{array}{l} 2 \xrightarrow{4(3)} 15 \quad \Delta x_4 \Delta x_8 \Delta x_{12} \\ 3 \begin{cases} \xrightarrow{4(1)} 1 & \Delta x_0 \\ \xrightarrow{4(4)} 14 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases} \\ 4 \xrightarrow{4(2)} 13 \quad \Delta x_8 \Delta x_{12} \\ 5 \begin{cases} \xrightarrow{4(2)} 3 & \Delta x_0 \Delta x_4 \\ \xrightarrow{4(4)} 14 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases} \\ 6 \begin{cases} \xrightarrow{4(1)} 2 & \Delta x_4 \\ \xrightarrow{4(3)} 15 & \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases} \\ 7 \begin{cases} \xrightarrow{4(2)} 3 & \Delta x_0 \Delta x_4 \\ \xrightarrow{4(3)} 12 & \Delta x_0 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(3)} 13 & \Delta x_0 \Delta x_8 \Delta x_8 \\ \xrightarrow{4(4)} 14 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases} \\ 8 \xrightarrow{4(1)} 9 \quad \Delta x_{12} \\ 9 \begin{cases} \xrightarrow{4(3)} 7 & \Delta x_0 \Delta x_4 \Delta x_8 \\ \xrightarrow{4(4)} 14 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases} \\ 10 \begin{cases} \xrightarrow{4(2)} 6 & \Delta x_4 \Delta x_8 \\ \xrightarrow{4(3)} 15 & \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases} \\ 11 \begin{cases} \xrightarrow{4(2)} 5 & \Delta x_0 \Delta x_8 \\ \xrightarrow{4(3)} 12 & \Delta x_0 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(3)} 13 & \Delta x_0 \Delta x_8 \Delta x_{12} \end{cases} \\ 12 \begin{cases} \xrightarrow{4(1)} 6 & \Delta x_8 \\ \xrightarrow{4(2)} 13 & \Delta x_8 \Delta x_{12} \end{cases} \\ 13 \begin{cases} \xrightarrow{4(2)} 6 & \Delta x_4 \Delta x_8 \\ \xrightarrow{4(2)} 11 & \Delta x_4 \Delta x_{12} \\ \xrightarrow{4(3)} 15 & \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases} \\ 14 \begin{cases} \xrightarrow{4(2)} 6 & \Delta x_4 \Delta x_8 \\ \xrightarrow{4(2)} 11 & \Delta x_4 \Delta x_{12} \\ \xrightarrow{4(3)} 15 & \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases} \end{array}$$

$$\begin{array}{l}
15 \left\{ \begin{array}{l} \xrightarrow{4(2)} 5 \quad \Delta x_0 \Delta x_8 \\ \xrightarrow{4(3)} 7 \quad \Delta x_0 \Delta x_4 \Delta x_8 \\ \xrightarrow{4(3)} 10 \quad \Delta x_0 \Delta x_4 \Delta x_{12} \\ \xrightarrow{4(3)} 11 \quad \Delta x_0 \Delta x_4 \Delta x_{12} \\ \xrightarrow{4(3)} 12 \quad \Delta x_0 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(3)} 13 \quad \Delta x_0 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 14 \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{array} \right. \quad \begin{array}{l} 11 \left\{ \begin{array}{l} \xrightarrow{4(3)} 7 \quad \Delta x_0 \Delta x_4 \Delta x_8 \\ \xrightarrow{4(2)} 8 \quad \Delta x_0 \Delta x_{12} \\ \xrightarrow{4(2)} 9 \quad \Delta x_0 \Delta x_{12} \\ \xrightarrow{4(4)} 14 \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{array} \right.
\end{array}$$

3.2 Eight Round $GFSP_4$

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

$$1 \left\{ \begin{array}{l} \xrightarrow{4(4)} 14 \left\{ \begin{array}{l} \xrightarrow{4(2)} 6, \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \Delta x_{20} \Delta x_{24} \\ \xrightarrow{4(2)} 11, \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \Delta x_{20} \Delta x_{28} \\ \xrightarrow{4(3)} 15, \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \Delta x_{20} \Delta x_{24} \Delta x_{28} \end{array} \right. \\ \xrightarrow{4(4)} 15 \left\{ \begin{array}{l} \xrightarrow{4(2)} 5, \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \Delta x_{16} \Delta x_{24} \\ \xrightarrow{4(3)} 7, \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \Delta x_{16} \Delta x_{20} \Delta x_{24} \\ \xrightarrow{4(3)} 10(11), \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \Delta x_{16} \Delta x_{20} \Delta x_{24} \\ \xrightarrow{4(3)} 12(13), \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \Delta x_{16} \Delta x_{24} \Delta x_{28} \\ \xrightarrow{4(4)} 14(15), \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \Delta x_{16} \Delta x_{20} \Delta x_{24} \Delta x_{28} \end{array} \right. \end{array} \right.$$

We show the minimum number of differential active s -boxes for 8-round $GFSP_4$ is equal or larger 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 $\Delta y = \Delta x \oplus \Delta z$, we have $H_w(\Delta y) \leq H_w(\Delta x) + H_w(\Delta z)$. Let $\Delta y_i = F(x) \oplus F(x \oplus \Delta x_i)$. From the structure of 8-round $GFSP_4$, we have

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

From the definition of branch number P_d , we have

$$H_w(\Delta y_i) + H_w(\Delta x_i) \geq P_d$$

Therefore, we have

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

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

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

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:

$$\begin{aligned}
5 &\begin{cases} N_5(S) \geq P_d + 1, & 5 \xrightarrow{4(2)} 3 \xrightarrow{4(1)} 1, \Delta x_4 \Delta x_8 \Delta x_{16} \\ N_5(S) \geq 2P_d + 1, & \text{else} \end{cases} \\
6 &\begin{cases} N_6(S) \geq P_d + 2, & 6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15, \Delta x_4 \Delta x_{20} \Delta x_{24} \Delta x_{28} \\ N_6(S) \geq 2P_d + 1, & \text{else} \end{cases} \\
7 &\begin{cases} N_7(S) \geq P_d + 1, & 7 \xrightarrow{4(2)} 3 \xrightarrow{4(1)} 1, \Delta x_0 \Delta x_4 \Delta x_{16} \\ N_7(S) \geq P_d + 2, & 7 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4, \Delta x_0 \Delta x_8 \Delta x_{12} \Delta x_{24} \\ N_7(S) \geq P_d + 3, & 7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13, \Delta x_0 \Delta x_8 \Delta x_{12} \Delta x_{24} \Delta x_{28} \\ N_6(S) \geq 2P_d + 1, & \text{else} \end{cases} \\
9 &\begin{cases} N_9(S) \geq P_d + 3, & 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3, \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{16} \Delta x_{20} \\ N_6(S) \geq 2P_d + 1, & \text{else} \end{cases} \\
10 &\begin{cases} N_{10}(S) \geq P_d + 3, & 10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15, \Delta x_4 \Delta x_8 \Delta x_{20} \Delta x_{24} \Delta x_{28} \\ N_{10}(S) \geq P_d + 1, & 10 \xrightarrow{4(2)} 6 \xrightarrow{4(1)} 2, \Delta x_4 \Delta x_8 \Delta x_{20} \\ N_6(S) \geq 2P_d + 1, & \text{else} \end{cases} \\
11 &\begin{cases} N_{11}(S) \geq P_d + 3, & 11 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3, \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{16} \Delta x_{20} \\ N_{11}(S) \geq P_d + 1, & 11 \xrightarrow{4(2)} 8 \xrightarrow{4(1)} 9, \Delta x_0 \Delta x_{12} \Delta x_{28} \\ N_6(S) \geq 2P_d + 1, & \text{else} \end{cases} \\
12 &\begin{cases} N_{12}(S) \geq P_d + 2, & 12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15, \Delta x_8 \Delta x_{20} \Delta x_{24} \Delta x_{28} \\ N_6(S) \geq 2P_d + 1, & \text{else} \end{cases}
\end{aligned}$$

$$\begin{array}{l}
13 \left\{ \begin{array}{l}
N_{13}(S) \geq P_d + 2, \quad 13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3, \quad \Delta x_0 \Delta x_8 \Delta x_{16} \Delta x_{20} \\
N_{13}(S) \geq P_d + 2, \quad 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4, \quad \Delta x_0 \Delta x_8 \Delta x_{12} \Delta x_{24} \\
N_{13}(S) \geq P_d + 3, \quad 13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13, \quad \Delta x_0 \Delta x_8 \Delta x_{12} \Delta x_{24} \Delta x_{28} \\
N_{13}(S) \geq 2P_d + 1, \text{ else}
\end{array} \right. \\
14 \left\{ \begin{array}{l}
N_{13}(S) \geq P_d + 3, \quad 14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15, \quad \Delta x_4 \Delta x_8 \Delta x_{20} \Delta x_{24} \Delta x_{28} \\
N_{14}(S) \geq P_d + 1, \quad 14 \xrightarrow{4(2)} 6 \xrightarrow{4(1)} 2, \quad \Delta x_4 \Delta x_8 \Delta x_{20} \\
N_{14}(S) \geq P_d + 2, \quad 14 \xrightarrow{4(2)} 11 \xrightarrow{4(2)} 8(9), \quad \Delta x_4 \Delta x_{12} \Delta x_{16} \Delta x_{28} \\
N_{13}(S) \geq 2P_d + 1, \text{ else}
\end{array} \right. \\
15 \left\{ \begin{array}{l}
N_{15}(S) \geq P_d + 2, \quad 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3, \quad \Delta x_0 \Delta x_8 \Delta x_{16} \Delta x_{20} \\
N_{15}(S) \geq P_d + 2, \quad 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3, \quad \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{16} \Delta x_{20} \\
N_{15}(S) \geq P_d + 3, \quad 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8(9), \quad \Delta x_0 \Delta x_4 \Delta x_{12} \Delta x_{16} \Delta x_{28} \\
N_{15}(S) \geq P_d + 2, \quad 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4, \quad \Delta x_0 \Delta x_8 \Delta x_{12} \Delta x_{24} \\
N_{15}(S) \geq P_d + 3, \quad 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13, \quad \Delta x_0 \Delta x_8 \Delta x_{12} \Delta x_{24} \Delta x_{28} \\
N_{15}(S) \geq 2P_d + 1, \text{ else}
\end{array} \right.
\end{array}$$

From the above discussion, we get the following Lemma.

Lemma 1. *If round function are permutation, the minimum number of differential active s-boxes for 8-round GFSP₄ scheme is equal or larger than $P_d + 1$.*

3.3 Sixteen Round GFSP₄

Theorem 2. *If round functions are permutations, the minimum number of differential active s-boxes for 16-round GFSP₄ scheme is equal or larger than $3P_d + 1$.*

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

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

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 $N_8(S) \geq 2P_d$, 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.

$$\begin{array}{ll}
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.
\end{array}$$

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

$$\begin{aligned}
\Delta y_0 &= \Delta x_1 \oplus \Delta x_4, & \Delta y_4 &= \Delta x_2 \oplus \Delta x_8, \\
\Delta y_8 &= \Delta x_3 \oplus \Delta x_{12}, & \Delta y_{12} &= \Delta x_0 \oplus \Delta x_{16}, \\
\Delta y_{16} &= \Delta x_4 \oplus \Delta x_{20}, & \Delta y_{20} &= \Delta x_8 \oplus \Delta x_{24}, \\
\Delta y_{24} &= \Delta x_{12} \oplus \Delta x_{28}, & \Delta y_{28} &= \Delta x_{16} \oplus \Delta x_{32}, \\
\Delta y_{32} &= \Delta x_{20} \oplus \Delta x_{36}, & \Delta y_{36} &= \Delta x_{24} \oplus \Delta x_{40}, \\
\Delta y_{40} &= \Delta x_{28} \oplus \Delta x_{44}, & \Delta y_{44} &= \Delta x_{32} \oplus \Delta x_{48}, \\
\Delta y_{48} &= \Delta x_{36} \oplus \Delta x_{52}, & \Delta y_{52} &= \Delta x_{40} \oplus \Delta x_{54}, \\
\Delta y_{56} &= \Delta x_{44} \oplus \Delta x_{60}, & \Delta y_{60} &= \Delta x_{48} \oplus \Delta x_{64}.
\end{aligned}$$

Form the definition of branch number P_d , If $\Delta x_i \neq 0$, then

$$H_w(\Delta y_i) + H_w(\Delta x_i) \geq P_d$$

Therefore, we have

$$\text{If } \Delta x_0 \neq 0, \text{ then } H_w(\Delta x_0) + H_w(\Delta x_1) + H_w(\Delta x_4) \geq P_d.$$

$$\text{If } \Delta x_4 \neq 0, \text{ then } H_w(\Delta x_2) + H_w(\Delta x_4) + H_w(\Delta x_8) \geq P_d.$$

$$\text{If } \Delta x_8 \neq 0, \text{ then } H_w(\Delta x_3) + H_w(\Delta x_8) + H_w(\Delta x_{12}) \geq P_d.$$

$$\text{If } \Delta x_{12} \neq 0, \text{ then } H_w(\Delta x_0) + H_w(\Delta x_{12}) + H_w(\Delta x_{16}) \geq P_d.$$

$$\text{If } \Delta x_{16} \neq 0, \text{ then } H_w(\Delta x_4) + H_w(\Delta x_{16}) + H_w(\Delta x_{20}) \geq P_d.$$

$$\text{If } \Delta x_{20} \neq 0, \text{ then } H_w(\Delta x_8) + H_w(\Delta x_{20}) + H_w(\Delta x_{24}) \geq P_d.$$

$$\text{If } \Delta x_{24} \neq 0, \text{ then } H_w(\Delta x_{12}) + H_w(\Delta x_{24}) + H_w(\Delta x_{32}) \geq P_d.$$

$$\text{If } \Delta x_{28} \neq 0, \text{ then } H_w(\Delta x_{16}) + H_w(\Delta x_{28}) + H_w(\Delta x_{32}) \geq P_d.$$

$$\text{If } \Delta x_{32} \neq 0, \text{ then } H_w(\Delta x_{20}) + H_w(\Delta x_{32}) + H_w(\Delta x_{36}) \geq P_d.$$

$$\text{If } \Delta x_{36} \neq 0, \text{ then } H_w(\Delta x_{24}) + H_w(\Delta x_{36}) + H_w(\Delta x_{40}) \geq P_d.$$

$$\text{If } \Delta x_{40} \neq 0, \text{ then } H_w(\Delta x_{28}) + H_w(\Delta x_{40}) + H_w(\Delta x_{44}) \geq P_d.$$

$$\text{If } \Delta x_{44} \neq 0, \text{ then } H_w(\Delta x_{32}) + H_w(\Delta x_{44}) + H_w(\Delta x_{48}) \geq P_d.$$

$$\text{If } \Delta x_{48} \neq 0, \text{ then } H_w(\Delta x_{36}) + H_w(\Delta x_{48}) + H_w(\Delta x_{52}) \geq P_d.$$

$$\text{If } \Delta x_{52} \neq 0, \text{ then } H_w(\Delta x_{40}) + H_w(\Delta x_{52}) + H_w(\Delta x_{56}) \geq P_d.$$

$$\text{If } \Delta x_{56} \neq 0, \text{ then } H_w(\Delta x_{44}) + H_w(\Delta x_{56}) + H_w(\Delta x_{60}) \geq P_d.$$

$$\text{If } \Delta x_{60} \neq 0, \text{ then } H_w(\Delta x_{48}) + H_w(\Delta x_{60}) + H_w(\Delta x_{64}) \geq P_d.$$

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 $\Delta x_0 \Delta x_{12} \Delta x_{28} \Delta x_{32} \Delta x_{36} \Delta x_{40} \Delta x_{48} \Delta x_{52}$, and $\Delta x_4 = \Delta x_8 = \Delta x_{16} = \Delta x_{20} = \Delta x_{24} = \Delta x_{44} = \Delta x_{56} = \Delta x_{60} = 0$. Hence, the number of active boxes is

$$\begin{aligned} & H_w(\Delta x_0) + H_w(\Delta x_{12}) + H_w(\Delta x_{28}) + H_w(\Delta x_{32}) + H_w(\Delta x_{36}) + H_w(\Delta x_{40}) \\ & \quad + H_w(\Delta x_{48}) + H_w(\Delta x_{52}) \\ &= [H_w(\Delta x_0) + H_w(\Delta x_{12})] + H_w(\Delta x_{28}) + [H_w(\Delta x_{32}) + H_w(\Delta x_{36})] + \\ & \quad [H_w(\Delta x_{40}) + H_w(\Delta x_{52})] + H_w(\Delta x_{48}) \\ &\geq P_d + P_d + P_d + 2 = 3P_d + 2 \end{aligned}$$

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 $\{s_{11}, s_{12}, s_{13}, s_{14}, s_{21}, \dots, s_{16,4}\}$. If the round functions are permutations, then, the maximum differential/linear characteristic probabilities of 16-round GFSP₄ 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 $GFSP^{(f_{11}, f_{12}, \dots, f_{rm})}$ hereafter, where $f_{ij} (i = 1, \dots, r, j = 1, \dots, m)$ are rm independent random functions from $\{0, 1\}^l$ to $\{0, 1\}^l$. We first present some 7-round distinguishers.

Choose

$$\begin{aligned} x_3 &= (x, a_{3,2}, \dots, a_{3,m}), & x_2 &= (a_{2,1}, a_{2,2}, \dots, a_{2,m}), \\ x_1 &= (a_{1,1}, a_{1,2}, \dots, a_{1,m}), & x_0 &= (a_{0,1}, a_{0,2}, \dots, a_{0,m}). \end{aligned}$$

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:

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

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

In the 4th round a transformation on $x_{12} = (x \oplus a_{12,1}, a_{12,2}, \dots, a_{12,m})$ using F_4 is as follows:

$$x_{12} = (x \oplus a_{12,1}, a_{12,2}, \dots, a_{12,m}) \xrightarrow{F_4} (\theta_{11}y \oplus b_1, \theta_{11}y \oplus b_2, \dots, \theta_{11}y \oplus b_m)$$

where $y = f_{41}(x \oplus a_{12,1})$, $b_j (1 \leq j \leq m)$ are entirely determined by $a_{12,j} (2 \leq j \leq m)$ and $f_{4j} (2 \leq j \leq m)$, thus $b_j (1 \leq j \leq m)$ are constants when $f_{4j} (2 \leq j \leq m)$ are fixed. Therefore, the input of the 5th round is

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

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

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

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 $x_0 = x_0^*, x_1 = x_1^*, x_2 = x_2^*, x_{3,1} \neq x_{3,1}^*, x_{3,j} = x_{3,j}^* (2 \leq j \leq m)$, then for any subset $I \subseteq \{1, 2, \dots, m\}$, 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 $f_{11}, \dots, f_{1m}, f_{21}, \dots, f_{7m}$ 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 $f = GFSP(f_{11}, f_{12}, \dots, f_{7m})$. There exists a non-adaptive distinguisher \mathcal{A} with q queries such that:*

$$Adv_{\mathcal{A}} \geq 1 - 2^{-\frac{n(m-1)}{8}}$$

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 $x_0 = x_0^*, x_1 = x_1^*, x_2 = x_2^*, x_{3,1} \neq x_{3,1}^*, x_{3,j} = x_{3,j}^* (2 \leq j \leq m)$.
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 $1 \leq j_1 < j_2 \leq m$,

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

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 $f = GFSP(f_{11}^*, f_{12}^*, \dots, f_{7m}^*)$. Using lemma 2, we get $p_1 = 1$. Therefore, we obtained that

$$Adv_{\mathcal{A}}(f, f^*) \geq 1 - 2^{-\frac{n(m-1)}{8}}$$

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 $f_{11}^*, \dots, f_{1m}^*, f_{21}^*, \dots, f_{8m}^*$ 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 $f = GFSP(f_{11}^*, f_{12}^*, \dots, f_{8m}^*)$. If the branch number of linear transformation $P : (\{0, 1\}^l)^m \rightarrow (\{0, 1\}^l)^m$ is $m + 1$, then for any adaptive distinguisher \mathcal{A} with q queries we have*

$$Adv_{\mathcal{A}}(f, f^*) \leq 13q^2 2^{-\frac{n}{4}}$$

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

We denote the $(x_k^i)_{i \in [1, \dots, q]}$ and $(y_k^i)_{i \in [1, \dots, q]}$ 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 i th round, and let $x_j = (x_{j,1}, \dots, x_{j,m})$. 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 $\mathcal{X} = I_n^\neq$, $\mathcal{Y} = (Y^1, \dots, Y^q) = \{(y_3^i, y_2^i, y_1^i, y_0^i)_{i \in [1, \dots, q]} \mid (y_3^{[1 \sim q]} \in I_{\frac{n}{4}}^\neq) \wedge (y_2^{[1 \sim q]} \in I_{\frac{n}{4}}^\neq) \wedge (y_1^{[1 \sim q]} \in I_{\frac{n}{4}}^\neq) \wedge (y_0^{[1 \sim q]} \in I_{\frac{n}{4}}^\neq)\}$. We want to establish a lower bound on the size of \mathcal{Y} and the $Pr[X \rightarrow Y]$ 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:

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

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

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

$$\begin{aligned} Pr[X \rightarrow Y] &= Pr[Y^i = (y_3^i, y_2^i, y_1^i, y_0^i) = (x_{35}^i, x_{34}^i, x_{33}^i, x_{32}^i), i = 1, \dots, q] \\ Y^i &= (x_{35}^i, x_{34}^i, x_{33}^i, x_{32}^i) \text{ if and only if} \end{aligned}$$

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

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

$$\begin{aligned} Pr[X \rightarrow Y] &= Pr[Y^i = (y_3^i, y_2^i, y_1^i, y_0^i) = (x_{35}^i, x_{34}^i, x_{33}^i, x_{32}^i), i = 1, \dots, q] \\ &= Pr[A] \geq Pr[A|B]Pr[B] \end{aligned}$$

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

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

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 $Pr(x_{28}^i = x_{28}^j)$.

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

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 $(x_2^i, x_1^i, x_0^i) \neq (x_2^j, x_1^j, x_0^j)$

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

From $x_{12}^i = x_9^i \oplus F_3(x_8^i)$, the SP network of round function and $f_{31}, f_{32}, \dots, f_{3m}$ 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 $Pr(x_4^i = x_4^j) = \begin{cases} 0 & x_0^i = x_0^j \\ 2^{-\frac{n}{4}} & x_0^i \neq x_0^j \end{cases}$

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

From $x_8^i = x_5^i \oplus F_2(x_4^i)$, the SP network of round function and $f_{21}, f_{22}, \dots, f_{2m}$ 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 round *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 focused 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 7-round *GFSP*, then point out 7-round *GFSP* is not pseudorandom for non-adaptive adversary. Finally, we prove 8-round *GFSP* is pseudorandom for any adversaries.

References

1. E.Biham, A.Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology*, 1991,4(1),3-72.
2. M.Matsui, "Linear cryptanalysis method for DES cipher, Advances in Cryptology-Eurocrypt'93 Proc., Berlin, Springer-Verlag, 1994, 386-397.

3. K.Nyberg. Perfect Nonlinear S-boxes. In Advances in Cryptology, EUROCRYPT'91,Brighton, England, Lecture Notes in Computer Science 547,pp.378-385, Springer-Verlag, Berlin,1991.
4. L.R.Knudsen, Practically secure Feistel ciphers," Fast Software Encryption,New York, Springer-Verlag,1994,211-221.
5. F.Chabaud, S. Vaudenay. Links between Differential and Linear Cryptanalysis. In Advances in Cryptology, EUROCRYPT'94, Perugia, Italy, Lecture Notes in Computer Science 950,pp.356-365, Springer-Verlag, Berlin,1995.
6. K.Nyberg,L.R.Knudsen,Provable Security Against a Differential Attack, Journal of Cryptology, Vol.8,No.1,27-37,1995.
7. M.Kanda, Practical security evaluation against differential and linear attacks for Feistel ciphers with SPN round function, SAC'2000 Proc., Berlin, Springer-Verlag,2000,168-179.
8. M. Luby and C. Rackoff, " How to construct pseudorandom permutations from pseudorandom functions," SIAM Journal on Computing, Vol.17,No.2,(1988),pp.373-386.(A preliminary version including other results appeared in Proceedings of the 18th ACM Symposium on Theory of Computing,(1986),pp.356-363).
9. U.M.Maurer, "A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators," Advances in Cryptology-Eurocrypt'92, Lecture Notes in Computer Science, Vol.658,pp.239-255,Springer-Verlag,1992.
10. Y.Zheng, T.Matsumoto, and H. Imai, "On the construction of block ciphers provably secure and not relying on any unproved hypotheses," Advances in Crypto'89, Lecture Notes in Computer Science, pp.461-480,Springer-Verlag,1989.
11. J.Patarin, " How to construct pseudorandom permutations from a single pseudorandom function," Advances in Cryptology-Eurocrypt'92, Lecture Notes in Computer Science, Vol.658,pp.256-266,Springer-Verlag,1992.
12. S.Lucks, " Faster Luby-Rackoff ciphers," Fast Software Encryption, Lecture Notes in Computer Science, Vol.1039,pp.189-203,Springer-Verlag,1996.
13. S.Patel, Z. Ramzan, and G. Sundaram, " Towards making Luby-Rackoff ciphers optimal and practical," Fast Software Encryption, Lecture Notes in Computer Science, Vol.1636, pp.171-185,Springer-Verlag,1999.
14. 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.
15. T.Iwata and K. Kurosawa, "On the Pseudorandomness of the AES Finalists-RC6 and Serpent", FSE2000, LNCS 1978,pp.231-243.
16. Z.Ramzan and L.Reyzin, " On the round security of symmetric-key cryptographic primitives", Advances in Cryptology-CRYPTO2000, LNCS 1880,p.376-393.??
17. H. Gilbert and M.Minier, "New Results on the Pseudorandomness of Some Block-cipher Constructions," FSE2001, LNCS 2355, pp.248-266.
18. T.Iwata, T.Yoshino, T.Yuasa and K. Kurosawa,"Round Security and Super-Pseudorandomness of MISTY Type Structure", FSE2001, LNCS 2355,pp.233-247.
19. Ju-Sung Kang,Sang-Uk Shin,Dowon Hong, and Okyeon Yi. Provable Security of KASUMI and 3GPP Encryption Mode f8. Advances in Cryptology—ASIACRYPT 2001, LNCS 2248, p:255-271,Springer-Verlag,2001.
20. L.R.Knudsen, "The security of Feistel ciphers with six rounds or less," Journal of Cryptology, Vol.15, No.3, pp.207-222,2002.
21. T.Iwata and K.Kurosawa, On the Correctness of Security Proofs for the 3GPP Confidentiality and Integrity Algorithms, Cryptography and Coding 2003,LNCS 2898,pp.306-318,2003

22. S.Moriai and S. Vaudenay, " On the Pseudorandomness of Top-Level Schemes of Block Ciphers",Advances in Cryptology—ASIACRYPT 2000,Springer-Verlag, Berlin,2000.
23. S. Vaudenay, " On Provable Security of Conventional Cryptography," In Information Security and Cryptography ICISC'99,Seoul,Korea, LNCS 1787,pp.1-16, Springer-Verlag, Berlin,1999.