Constructing S-boxes for Lightweight Cryptography with Feistel Structure

Yongqiang Li and Mingsheng Wang

The State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
yongq.lee@gmail.com
wangmingsheng@iie.ac.cn

Abstract. Differential uniformity and nonlinearity are two basic properties of S-boxes, which measure the resistance of S-boxes to differential and linear attack respectively. Besides these two properties, the hardware cost of S-boxes is also an important property which should be considered primarily in a limited resource environment. By use of Feistel structure, we investigate the problem of constructing S-boxes with excellent cryptographic properties and low hardware implementation cost in the present paper. Feistel structure is a widely used structure in the design of block ciphers, and it can be implemented easily in hardware. Three-round Feistel structure has been used to construct S-boxes in symmetric algorithms, such as CS-Ciper, CRYPTON and ZUC. In the present paper, we investigate the bounds on differential uniformity and nonlinearity of S-boxes constructed with three-round Feistel structure. By choosing suitable round functions, we show that for odd k, differential 4-uniform S-boxes over $\mathbb{F}_{2^k}^2$ with the best known nonlinearity can be constructed via three-round Feistel structure. Some experiment results are also given which show that optimal 4-bit S-boxes can be constructed with 4 or 5 round unbalanced Feistel structure.

Keywords: lightweight cryptography, S-boxes, Feistel structure, differential uniformity, nonlinearity.

1 Introduction

S-box is an important component of symmetric cryptography algorithms since it provides "confusion" for algorithms and in most cases is the only nonlinear part of round functions. S-boxes used in cryptography should posses good properties to resist various attacks. As a nonlinear part, an S-box usually takes a relative high cost in hardware implementation. Thus the cost of hardware implementation of an S-box is also of significant importance in lightweight cryptography algorithms, which are aiming to provide security in a limited resource environment. With the rapid development of lightweight cryptography, it is of particular interest to investigate the problem of constructing S-boxes with excellent cryptographic properties and low cost hardware implementation.

L. Batina and M. Robshaw (Eds.): CHES 2014, LNCS 8731, pp. 127–146, 2014.

Feistel structure is a well-known and widely used structure in symmetric cryptography. There are too many block ciphers designed with the scheme, and the most famous one among them is Data Encryption Standard (DES). Feistel structure is also used for constructing components of block ciphers. For example, MISTY used three-round Feistel structure to construct its nonlinear part FI [20]. The S-boxes in CS-Ciper [24], CRYPTON [18] and ZUC [25] are also constructed with three-round Feistel structure.

In general, the cost of hardware implementation of nonlinear functions is in direct proportion to its input and output size. For example, the 8-bit S-box of AES cost around 200 gates [5], and optimal 4-bit S-boxes cost less than 40 gates [17]. Thus, implementing functions on $\mathbb{F}_{2^k}$ often cost much less area than implementing functions on $\mathbb{F}_{2^{2k}}$. An advantage of constructing S-boxes over $\mathbb{F}_{2^k}^2$ with Feistel structure is that it only need to implement round functions on $\mathbb{F}_{2^k}$. Therefore, comparing with $2k$-bit S-boxes constructed directly with permutation polynomials over $\mathbb{F}_{2^{2k}}$, S-boxes over $\mathbb{F}_{2^k}^2$ constructed via Feistel structure with round functions on $\mathbb{F}_{2^k}$ cost much less area in hardware implementation.

However, the best cryptographic performance of S-boxes constructed with Feistel structure is not known clearly. Differential uniformity and nonlinearity are two basic properties of S-boxes, which measure the resistance of S-boxes to differential and linear attack respectively. S-boxes with lower differential uniformity and higher nonlinearity posses better resistance to differential and linear attack. Then it is interesting to investigate the lower bound and upper bound of differential uniformity and nonlinearity of S-boxes constructed with Feistel structure respectively.

There are already some work on the provable security of Feistel structure, such as [19,21]. Based on the assumption that round keys are independent and uniformly random, it is proven that the average differential uniformity of all permutations constructed via r-round ($r \geq 3$) Feistel structure with round permutation f and all possible round keys is less than or equal to $\Delta(f)^2$ [21]. Note that the bound is an average bound over all round keys, then for some fixed round keys, the differential uniformity of the corresponding permutation may larger than the above bound. This has been verified with experiment results in [1].

In the present paper, we mainly investigate the problem of constructing S-boxes with low differential uniformity, high nonlinearity and easy hardware implementation by use of Feistel structure. Without any statistical assumptions, we investigate the lower bound and upper bound of S-boxes constructed with three-round Feistel structure. We show that differential 4-uniform permutations with the best known nonlinearity can be constructed with three-round Feistel structure. It is also shown that optimal 4-bit S-boxes can be constructed with 4 and 5 round unbalanced Feistel structure.

The paper is organized as follows. In Sect. 2, some preliminaries are given. In Sect. 3, the bound on differential uniformity and nonlinearity of S-boxes constructed with three-round Feistel structure is characterized. In Sect. 4, a class of differential 4-uniform permutations with the best known nonlinearity

over $\mathbb{F}_{2^{2k}}$ for odd k is constructed via three-round Feistel structure. In Sect. 5, it is shown that optimal 4-bit S-boxes can be constructed with unbalanced Feistel structure. A conclusion is given in Sect. 6.

2 Preliminaries

An S-box with n-bit input and output can be represented by a polynomial on the finite field $\mathbb{F}_{2^n}$. First, we introduce the definitions of differential uniformity, nonlinearity and algebraic degree.

Definition 1. *[22] Let $F(x) \in \mathbb{F}_{2^n}[x]$. The differential uniformity of $F(x)$ is defined as*

$$\Delta(F) = \max\{|R_F(a,b)| : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\},$$

where $R_F(a,b)$ means the set of solutions of equation $F(x) + F(x+a) = b$ in $\mathbb{F}_{2^n}$.

$F(x)$ is called differential δ-uniform when $\Delta(F) = \delta$. It is easy to see that the lower bound on differential uniformity of $F(x) \in \mathbb{F}_{2^n}[x]$ is 2. Differential 2-uniform functions are called almost perfect nonlinear (APN). The differential spectrum is the set $\{|R_F(a,b)| : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}$.

Definition 2. *Let $F(x) \in \mathbb{F}_{2^n}[x]$. The minimum distance of the components of $F(x)$ and all affine Boolean functions on n variables is called the nonlinearity of $F(x)$. It is denoted by $\mathcal{NL}(F)$ and can be computed as follows*

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2}\Lambda(F),$$

where $\Lambda(F) = \max\{|\lambda_F(a,b)| : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*\}$ *and* $\lambda_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bF(x)+ax)}$.

For odd n and $F(x) \in \mathbb{F}_{2^n}[x]$, it holds that $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ [10]. For even n and $F(x) \in \mathbb{F}_{2^n}[x]$, the upper bound on the nonlinearity of $F(x)$ is still open, and the best known nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$ [11].

Definition 3. *The algebraic degree of $G(x) = \sum_{j=0}^{2^n-1} c_j x^j \in \mathbb{F}_{2^n}[x]$, which is denoted by $d^\circ(G)$, equals the maximum hamming weight of binary expansion of j with $c_j \neq 0$. In other words, $d^\circ(G) = \max_{j,c_j \neq 0}\{\omega_2(j)\}$, where $\omega_2(j)$ means the number of nonzero terms in the binary expansion of j.*

For other cryptographic properties of Boolean functions and vectorial Boolean functions, one can see [8,9] for more details.

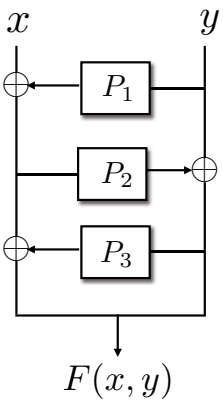

Fig. 1. An S-box constructed with three-round Feistel structure

3 On Properties of S-boxes Constructed with Three-Round Feistel Structure

Throughout this section, we consider S-boxes constructed with three-round Feistel structure as in Figure 1. Let $P_i(x) \in \mathbb{F}_{2^k}[x], 1 \leq i \leq 3$. Then an S-box over $\mathbb{F}_{2^k}^2$ constructed as in Figure 1 can be characterized as

$$F(x,y) = (x + P_1(y) + P_3(y + P_2(x + P_1(y))), y + P_2(x + P_1(y))).$$

We also write $F(x,y)$ as $F_{P_1,P_2,P_3}(x,y)$ when the sequence of round transformations P_1, P_2 and P_3 is emphasized. It is easy to see that $F(x,y)$ is a permutation over $\mathbb{F}_{2^k}^2$ and

$$F_{P_1,P_2,P_3}(x,y)^{-1} = F_{P_3,P_2,P_1}(x,y),$$

where $F_{P_1,P_2,P_3}(x,y)^{-1}$ means the compositional inverse of $F_{P_1,P_2,P_3}(x,y)$.

This construction has been used in CS-Ciper [24], CRYPTON [18] and ZUC [25]. In this section, we mainly investigate the bound on differential uniformity and nonlinearity of $F(x,y)$.

First, it needs the following result. Remember that for $F(x) \in \mathbb{F}_{2^n}[x]$, $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, $R_F(a,b)$ means $\{y \in \mathbb{F}_{2^n} \mid F(y) + F(y+a) = b\}$.

Lemma 1. *[6,1] Suppose $P_i(x) \in \mathbb{F}_{2^k}[x], 1 \leq i \leq 3$, and $F(x,y)$ be the S-box constructed as in Figure 1. Then the following statements hold.*

(1) Let $a,b,c \in \mathbb{F}_{2^k}$ and $(a,b) \neq (0,0)$. Then the equation $F(x,y) + F(x+a, y+b) = (c,0)$ has $|R_{P_1}(b, c+a)| \cdot |R_{P_2}(c,b)|$ roots in $\mathbb{F}_{2^k}^2$. Furthermore, these roots are $(z_i + P_1(y_j), y_j)$, where $y_j \in R_{P_1}(b, c+a)$ and $z_i \in R_{P_2}(c,b)$.
(2) Let $a,b \in \mathbb{F}_{2^k}$ and $c \in \mathbb{F}_{2^k}^*$. Then $\lambda_F((a,b),(0,c)) = \lambda_{P_1}(c+b,a)\lambda_{P_2}(a,c)$.

Theorem 1. *Suppose $P_i(x) \in \mathbb{F}_{2^k}[x], 1 \leq i \leq 3$, and $F(x,y)$ be the S-box constructed as in Figure 1. Then the following statements hold.*

(1) If $P_2(x)$ is not a permutation over $\mathbb{F}_{2^k}$, then $\Delta(F) \geq 2^{k+1}$.
(2) If $P_2(x)$ is a permutation over $\mathbb{F}_{2^k}$, then $\Delta(F) \geq 2\Delta(P_2)$.

Proof. (1). Since $P_2(x)$ is not a permutation over $\mathbb{F}_{2^k}$, then there exists $a \in \mathbb{F}_{2^k}^*$ such that

$$P_2(x) + P_2(x+a) = 0$$

has at least 2 roots in $\mathbb{F}_{2^k}$, which means $|R_{P_2}(a,0)| \geq 2$. Notice that $R_{P_1}(0,0) = \mathbb{F}_{2^k}$, Then according to (1) of Lemma 1, $F(x,y) + F(x+a,y) = (a,0)$ has at least

$$|R_{P_1}(0,0)| \cdot |R_{P_2}(a,0)| = 2^{k+1}$$

roots in $\mathbb{F}_{2^k}^2$, which implies $\Delta(F) \geq 2^{k+1}$.

(2). Firstly, we choose $b, c \in \mathbb{F}_{2^k}^*$, such that $|R_{P_2}(c,b)| = \Delta(P_2)$. Then we choose $a \in \mathbb{F}_{2^k}$, such that $R_{P_1}(b, c+a)$ is nonempty. This means $|R_{P_1}(b,c+a)| \geq 2$. Therefore, according to (1) of Lemma 1,

$$F(x,y) + F(x+a, y+b) = (c,0)$$

has $2\Delta(P_2)$ roots in $\mathbb{F}_{2^k}$. Hence $\Delta(F) \geq 2\Delta(P_2)$. □

Let

$$\lambda_k = \begin{cases} 2^{\frac{k+1}{2}} & k \text{ odd}, \\ 2^{\frac{k}{2}+1} & k \text{ even}. \end{cases}$$

For $F(x) \in \mathbb{F}_{2^k}[x]$, we assume it holds

$$\Lambda(F) \geq \lambda_k,$$

which is a bound accepted widely for $F(x) \in \mathbb{F}_{2^n}[x]$ with n even, although it is not proven yet. Then we have the following result concerning the nonlinearity of $F(x,y)$.

Theorem 2. *Suppose $P_i(x) \in \mathbb{F}_{2^k}[x], 1 \leq i \leq 3$, and $F(x,y)$ be the S-box constructed as in Figure 1. If for any $a \in \mathbb{F}_{2^k}^*$, there exists $b \in \mathbb{F}_{2^k}^*$ such that $|\lambda_{P_2}(a,b)| \geq \lambda_k$, then $\mathcal{NL}(F(x,y)) \leq 2^{2k-1} - \frac{\lambda_k^2}{2}$.*

Proof. We only need to prove $\Lambda(F(x,y)) \geq \lambda_k^2$. Choose $a \in \mathbb{F}_{2^k}^*, c \in \mathbb{F}_{2^k}$ such that

$$|\lambda_{P_1}(c,a)| = \Lambda(P_1).$$

According to the condition of P_2, there exists $b \in \mathbb{F}_{2^k}^*$ such that $|\lambda_{P_2}(a,b)| \geq \lambda_k$. Then according to (2) of Lemma 1, it holds

$$\lambda_F((a, b+c), (0,b)) = \lambda_{P_1}(c,a)\lambda_{P_2}(a,b).$$

Note that

$$\Lambda(F(x,y)) = \max\{|\lambda_F((u_1,u_2),(v_1,v_2))| : (u_1,u_2),(v_1,v_2) \in \mathbb{F}_{2^k}^2, (v_1,v_2) \neq (0,0)\},$$

Table 1. Properties of known 8-bit S-boxes constructed with three-round Feistel structure

Algorithm/S-box	Differential uniformity	Nonlinearity	Algebraic degree
CS-Ciper/P	16	96	5
CRYPTON/S_0, S_1	8	96	5
ZUC/S_0	8	96	5

then it holds

$$\begin{aligned} \Lambda(F(x,y)) &\geq |\lambda_F((a,b+c),(0,b))| \\ &= |\lambda_{P_1}(c,a)| \times |\lambda_{P_2}(a,b)| \\ &\geq \Lambda(P_1)\lambda_k \\ &\geq \lambda_k^2, \end{aligned}$$

and we complete the proof. □

As for 8-bit S-boxes, which are the most often usage size in real applications, we have the following result.

Theorem 3. *Suppose $F_{P_1,P_2,P_3}(x,y)$ is an S-box over $\mathbb{F}_{2^4}^2$ constructed by three-round Feistel structure with round functions $P_i(x) \in \mathbb{F}_{2^4}[x]$, $1 \leq i \leq 3$. Then the following statements hold.*

(1) $\Delta(F_{P_1,P_2,P_3}) \geq 8$.
(2) If $\Delta(F_{P_1,P_2,P_3}) = 8$, then $\mathcal{NL}(F_{P_1,P_2,P_3}) \leq 96$.

Proof. Notice that there are no APN permutations over $\mathbb{F}_{2^4}$ [16], then the differential uniformity of any permutation over $\mathbb{F}_{2^4}^2$ constructed with three-round Feistel structure is larger than or equal to 8.

If $\Delta(F_{P_1,P_2,P_3}) = 8$, then $P_2(x)$ is a differential 4-uniform permutation over $\mathbb{F}_{2^4}$ according to Theorem 1. By an exhaustive search, it can be checked that the condition of Theorem 2 is satisfied by all differential 4-uniform permutations over $\mathbb{F}_{2^4}$. Then according to Theorem 2, we have $\mathcal{NL}(F_{P_1,P_2,P_3}) \leq 96$. □

The permutation P in CS-Ciper, S-boxes S_0, S_1 in CRYPTON and an S-box S_0 in ZUC are constructed by three-round Feistel structure. The properties of these 8-bit S-boxes are listed in Table 1.

The permutation P in CS-Ciper is an involution over $\mathbb{F}_{2^4}^2$, which means $P(P(x,y)) = (x,y)$ for $(x,y) \in \mathbb{F}_{2^4}^2$. The differential uniformity of the permutation P in CS-Ciper does not achieve the bound in Theorem 3. In Example 1, we give an involution over $\mathbb{F}_{2^4}^2$, which achieves the bound in Theorem 3 and has a better algebraic degree.

According to Theorem 3, the differential uniformity and nonlinearity of S-boxes in CRYPTON and ZUC can not be improved by choosing different round transformations. However, the following example shows that the algebraic degree of S-boxes constructed with three-round Feistel structure can be improved to 6.

Example 1. Let $P_1(x) = x^3, P_2(x) = x + g^6x^{10} + g^3x^{13}$, where g is a root of $x^4 + x + 1 = 0$, and $P_3(x) = x^3 + (x^2 + x + 1)\mathrm{Tr}(x^3) = \sum_{i=4}^{14} x^i$. $P_1(x)$ is a case of Gold function [12,22], which is an APN polynomial. $P_2(x)$ is a differential 4-uniform permutation over $\mathbb{F}_{2^4}$ got by computer searching. $P_3(x)$ is an APN polynomial which is CCZ-equivalent and EA-inequivalent to $P_1(x)$ [3].

It is easy to check that F_{P_1,P_2,P_3} and F_{P_3,P_2,P_3} are S-boxes over $\mathbb{F}_{2^4}^2$ with differential uniformity 8, nonlinearity 96 and algebraic degree 6. Furthermore, F_{P_3,P_2,P_3} is an involution over $\mathbb{F}_{2^4}^2$.

4 Optimal S-boxes Constructed with Three Round Feistel Structure

When k is odd, the upper bound on nonlinearity of $F(x, y)$ in Theorem 2 is $2^{2k-1} - 2^k$, which is the best known nonlinearity of functions on $\mathbb{F}_{2^k}^2$. Furthermore, there exist APN permutations over $\mathbb{F}_{2^k}$ with k odd. Thus, it is possible to get differential 4-uniform permutations over $\mathbb{F}_{2^k}^2$ with the best known nonlinearity.

Suppose k is an odd integer, $\gcd(i, k) = 1$. Then x^{2^i+1} is an APN permutation over $\mathbb{F}_{2^k}$ and denote its compositional inverse by $x^{\frac{1}{2^i+1}}$. Let $F(x, y)$ be the S-box over $\mathbb{F}_{2^k}^2$ constructed by three-round Feistel structure with round functions $P_1(x) = P_3(x) = x^{2^i+1}$ and $P_2(x) = x^{\frac{1}{2^i+1}}$. Then

$$\begin{aligned} F(x, y) &= (x + y^{2^i+1} + (y + (x + y^{2^i+1})^{\frac{1}{2^i+1}})^{2^i+1}, y + (x + y^{2^i+1})^{\frac{1}{2^i+1}}) \\ &= (y^{2^i+1} + y^{2^i}(x + y^{2^i+1})^{\frac{1}{2^i+1}} + y(x + y^{2^i+1})^{\frac{2^i}{2^i+1}}, y + (x + y^{2^i+1})^{\frac{1}{2^i+1}}). \end{aligned}$$

In this section, we show that $F(x, y)$ constructed as above is a differential 4-uniform permutation over $\mathbb{F}_{2^k}^2$ with the best known nonlinearity.

In order to characterize the differential uniformity and nonlinearity of $F(x, y)$, we need the following lemmas firstly.

Lemma 2. *Suppose k is an odd integer and $\gcd(i, k) = 1$. Then for any $(b, d) \in \mathbb{F}_{2^k}^2$ with $(b, d) \neq (0, 0)$, the following system of equations*

$$\begin{cases} dy^{2^i} + d^{2^i}y + b^{2^i}z + bz^{2^i} = 0, \\ by^{2^i} + b^{2^i}y + (b + d)z^{2^i} + (b + d)^{2^i}z = 0 \end{cases}$$

has exactly 4 roots in $\mathbb{F}_{2^k}^2$. Furthermore, the following statements hold.

(1) If $bd(b + d) = 0$, then the 4 roots are $(0, 0), (0, \beta), (\beta, 0)$ and (β, β), where $\beta \in \{b, d\}$ with $\beta \neq 0$.
(2) If $bd(b + d) \neq 0$, then the 4 roots are $(0, 0)$, (d, b), $(b, b + d)$ and $(b + d, d)$.

Proof. To solve the following system of equations

$$\begin{cases} dy^{2^i} + d^{2^i}y + b^{2^i}z + bz^{2^i} = 0, & (1) \\ by^{2^i} + b^{2^i}y + (b+d)^{2^i}z + (b+d)z^{2^i} = 0, & (2) \end{cases}$$

we have the following cases.

First, if $b = 0$, then $d \neq 0$ and the above system of equations becomes

$$\begin{cases} dy^{2^i} + d^{2^i}y = 0, \\ dz^{2^i} + d^{2^i}z = 0. \end{cases}$$

It is easy to see that the above systems of equations has exactly 4 roots in $\mathbb{F}_{2^k}^2$, which are

$$(0,0), (0,d), (d,0), (d,d).$$

This is because $\alpha x^{2^i} + \alpha^{2^i}x$ is a linear mapping on $\mathbb{F}_{2^k}$ with kernel $\{0, \alpha\}$ for any $\alpha \in \mathbb{F}_{2^k}^*$, since $\gcd(i,k) = 1$.

The case of $d = 0, b \neq 0$, and $b = d \in \mathbb{F}_{2^k}^*$ can be proved similarly.

Next, we prove the case of $bd(b+d) \neq 0$, which is equivalent to $b, d \in \mathbb{F}_{2^k}^*$ and $b \neq d$. Let

$$A = b^2 + bd + d^2,$$

and

$$B = b^{2^i}d + bd^{2^i}.$$

Notice that k is odd, $\gcd(i,k) = 1$, $b, d \in \mathbb{F}_{2^k}^*$ and $b \neq d$, then $A \neq 0$ and $B \neq 0$. We add equation (1) multiplied by $b+d$ to equation (2) multiplied by b, from which we eliminate z^{2^i} and get

$$z = \frac{1}{B}(Ay^{2^i} + (b^{2^i+1} + bd^{2^i} + d^{2^i+1})y).$$

Substitute the above equality to equation (1) and multiply both sides by B^{2^i+1}, then we have

$$\begin{aligned} 0 &= dB^{2^i+1}y^{2^i} + d^{2^i}B^{2^i+1}y + (bB)^{2^i}(Ay^{2^i} + (b^{2^i+1} + bd^{2^i} + d^{2^i+1})y) \\ &\quad + bB(Ay^{2^i} + (b^{2^i+1} + bd^{2^i} + d^{2^i+1})y)^{2^i} \\ &= bBA^{2^i}y^{2^{2i}} + (dB^{2^i+1} + (bB)^{2^i}A + bB(b^{2^i+1} + bd^{2^i} + d^{2^i+1})^{2^i})y^{2^i} \\ &\quad + (d^{2^i}B^{2^i+1} + (bB)^{2^i}(b^{2^i+1} + bd^{2^i} + d^{2^i+1}))y \\ &= bBA^{2^i}y^{2^{2i}} + bA^{2^i}(b^{2^{2i}}d + bd^{2^{2i}})y^{2^i} + bA^{2^i}B^{2^i}y, \end{aligned} \quad (3)$$

where the coefficients of y^{2^i} and y is computed as follows. First, we have

$$\begin{aligned} dB^{2^i+1} &= d(b^{2^i}d + bd^{2^i})^{2^i+1} \\ &= b^{2^{2i}+2^i}d^{2^i+2} + b^{2^{2i}+1}d^{2^{i+1}+1} + b^{2^{i+1}}d^{2^{2i}+2} + b^{2^i+1}d^{2^{2i}+2^i+1}, \end{aligned}$$

$$\begin{aligned} (bB)^{2^i}A &= (b^{2^{2i}+2^i}d^{2^i} + b^{2^{i+1}}d^{2^{2i}})(b^2 + bd + d^2) \\ &= b^{2^{2i}+2^i+2}d^{2^i} + b^{2^{2i}+2^i+1}d^{2^i+1} + b^{2^{2i}+2^i}d^{2^i+2} \\ &\quad + b^{2^{i+1}+2}d^{2^{2i}} + b^{2^{i+1}+1}d^{2^{2i}+1} + b^{2^{i+1}}d^{2^{2i}+2}, \end{aligned}$$

and

$$\begin{aligned} bB(b^{2^i+1}+bd^{2^i}+d^{2^i+1})^{2^i} &= (b^{2^i+1}d+b^2d^{2^i})(b^{2^{2i}+2^i}+b^{2^i}d^{2^{2i}}+d^{2^{2i}+2^i}) \\ &= b^{2^{2i}+2^{i+1}+1}d+b^{2^{i+1}+1}d^{2^{2i}+1}+b^{2^i+1}d^{2^{2i}+2^i+1} \\ &\quad +b^{2^{2i}+2^i+2}d^{2^i}+b^{2^i+2}d^{2^{2i}+2^i}+b^2d^{2^{2i}+2^{i+1}}, \end{aligned}$$

then it holds

$$\begin{aligned} &dB^{2^i+1}+(bB)^{2^i}A+bB(b^{2^i+1}+bd^{2^i}+d^{2^i+1})^{2^i} \\ &= b^{2^{2i}+1}d^{2^{i+1}+1}+b^{2^{2i}+2^i+1}d^{2^i+1}+b^{2^{i+1}+2}d^{2^{2i}} \\ &\quad +b^{2^{2i}+2^{i+1}+1}d+b^{2^i+2}d^{2^{2i}+2^i}+b^2d^{2^{2i}+2^{i+1}} \\ &= b(b^{2^{2i}}d(d^{2^{i+1}}+b^{2^i}d^{2^i}+b^{2^{i+1}})+bd^{2^{2i}}(b^{2^{i+1}}+b^{2^i}d^{2^i}+d^{2^{i+1}})) \\ &= bA^{2^i}(b^{2^{2i}}d+bd^{2^{2i}}). \end{aligned}$$

The computation of the coefficient of y is easy.

$$\begin{aligned} &d^{2^i}B^{2^i+1}+(bB)^{2^i}(b^{2^i+1}+bd^{2^i}+d^{2^i+1}) \\ &= B^{2^i}(d^{2^i}(b^{2^i}d+bd^{2^i})+b^{2^i}(b^{2^i+1}+bd^{2^i}+d^{2^i+1})) \\ &= B^{2^i}(bd^{2^{i+1}}+b^{2^{i+1}+1}+b^{2^i+1}d^{2^i}) \\ &= bA^{2^i}B^{2^i}. \end{aligned}$$

Note that $b \neq 0$ and $A \neq 0$, then equation (3) is equivalent to

$$0 = (b^{2^i}d+bd^{2^i})y^{2^{2i}}+(b^{2^{2i}}d+bd^{2^{2i}})y^{2^i}+(b^{2^{2i}}d^{2^i}+b^{2^i}d^{2^{2i}})y.$$

Divid both sides by $d^{2^{2i}+2^i+1}$, then we have

$$\begin{aligned} 0 &= (\frac{b}{d}+(\frac{b}{d})^{2^i})(\frac{y}{d})^{2^{2i}}+(\frac{b}{d}+(\frac{b}{d})^{2^{2i}})(\frac{y}{d})^{2^i}+((\frac{b}{d})^{2^i}+(\frac{b}{d})^{2^{2i}})\frac{y}{d} \\ &= (\frac{b}{d}+(\frac{b}{d})^{2^i})((\frac{y}{d})^{2^i}+(\frac{y}{d}))^{2^i}+((\frac{b}{d})+(\frac{b}{d})^{2^i})^{2^i}((\frac{y}{d})^{2^i}+\frac{y}{d}). \end{aligned}$$

Notice that $\gcd(i,k)=1$, then $\alpha x^{2^i}+\alpha^{2^i}x$ is a linear polynomial on $\mathbb{F}_{2^k}$ with kernel $\{0,\alpha\}$ for any $\alpha \in \mathbb{F}_{2^k}^*$. Note that $\frac{b}{d}+(\frac{b}{d})^{2^i} \neq 0$, since $b,d \in \mathbb{F}_{2^k}^*$ and $b \neq d$. Therefore, it holds

$$(\frac{y}{d})^{2^i}+\frac{y}{d}=0$$

or

$$(\frac{y}{d})^{2^i}+\frac{y}{d}=\frac{b}{d}+(\frac{b}{d})^{2^i},$$

form which we get the roots of equation (3) are $y=0, y=d$ and $y=b, b+d$ respectively.

Substitute the values of y into equation (1) and equation (2), then one can solve and check that the roots of system of equation (1) and equation (2) are

$$(0,0),(d,b),(b,b+d),(b+d,d).$$

Then we complete the proof. □

Let $a \in \mathbb{F}_{2^k}^*$, denote $L_a(x) = ax^{2^i} + a^{2^i}x$ and take $\alpha \cdot \beta = \mathrm{Tr}(\alpha\beta)$ for inner product in $\mathbb{F}_{2^k}$, where $\mathrm{Tr}(x)$ is the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$. The adjoint linear mapping of $L_a(x)$, which is denoted by $L_a^*(x)$, is a linear mapping such that

$$\mathrm{Tr}(\beta L_a(\alpha)) = \mathrm{Tr}(L_a^*(\beta)\alpha)$$

for all $\alpha, \beta \in \mathbb{F}_{2^k}$. It is easy to see that

$$L_a^*(x) = a^{2^i}x + (ax)^{2^{n-i}}.$$

Lemma 2 means that

$$\mathcal{L}(y,z) = (L_d(y) + L_b(z), L_b(y) + L_{b+d}(z))$$

is a linear mapping on $\mathbb{F}_{2^k}^2$ with kernel dimension equals 2. Take $(\alpha,\beta)\cdot(y,z) = \mathrm{Tr}(\alpha y + \beta z)$ for inner product in $\mathbb{F}_{2^k}^2$, then we have

$$\begin{aligned}(\alpha,\beta)\cdot\mathcal{L}(y,z) &= (\alpha,\beta)\cdot(L_d(y)+L_b(z), L_b(y)+L_{b+d}(z))\\ &= \mathrm{Tr}(\alpha L_d(y) + \alpha L_b(z) + \beta L_b(y) + \beta L_{b+d}(z))\\ &= \mathrm{Tr}(L_d^*(\alpha)y + L_b^*(\beta)y + L_b^*(\alpha)z + L_{b+d}^*(\beta)z)\\ &= (L_d^*(\alpha)+L_b^*(\beta), L_b^*(\alpha)+L_{b+d}^*(\beta))\cdot(y,z).\end{aligned}$$

Hence it holds

$$\mathcal{L}^*(y,z) = (L_d^*(y) + L_b^*(z), L_b^*(y) + L_{b+d}^*(z)),$$

where $\mathcal{L}^*$ is the adjoint mapping of $\mathcal{L}$. By an elementary knowledge of linear algebra, we have

$$\dim(\ker(\mathcal{L}^*)) = \dim(\ker(\mathcal{L})) = 2.$$

Then the following result holds.

Lemma 3. *Suppose k is an odd integer and $\gcd(i,k) = 1$. Then for any $(b,d) \in \mathbb{F}_{2^k}^2$ with $(b,d) \neq (0,0)$, the following system of equations*

$$\begin{cases} d^{2^i}y + (dy)^{2^{n-i}} + b^{2^i}z + (bz)^{2^{n-i}} = 0,\\ b^{2^i}y + (by)^{2^{n-i}} + (b+d)^{2^i}z + ((b+d)z)^{2^{n-i}} = 0 \end{cases}$$

has exactly 4 roots in $\mathbb{F}_{2^k}^2$.

Theorem 4. *Suppose k is odd and $\gcd(i,k) = 1$. Let $F(x,y)$ be the S-box over $\mathbb{F}_{2^k}^2$ constructed by three-round Feistel structure with round functions $P_1(x) = P_3(x) = x^{2^i+1}$ and $P_2(x) = x^{\frac{1}{2^i+1}}$. Then the differential uniformity of $F(x,y)$ equals 4. Furthermore, the differential spectrum of $F(x,y)$ is $\{0,4\}$.*

Proof. Let $a,b,c,d \in \mathbb{F}_{2^k}$ and $(a,b) \neq (0,0)$. Then we need to prove that

$$F(x,y) + F(x+a, y+b) = (c,d)$$

has 0 or 4 roots in $\mathbb{F}_{2^k}^2$.

First, it is easy to see that the above equation is equivalent to the following system of equations

$$\begin{cases} by^{2^i} + b^{2^i}y + F^{'}(x,y) + F^{'}(x+a,y+b) = b^{2^i+1} + c, & (4) \\ (x+y^{2^i+1})^{\frac{1}{2^i+1}} + (x+a+(y+b)^{2^i+1})^{\frac{1}{2^i+1}} = b+d, & (5) \end{cases}$$

where

$$F^{'}(x) = y^{2^i}(x+y^{2^i+1})^{\frac{1}{2^i+1}} + y(x+y^{2^i+1})^{\frac{2^i}{2^i+1}}.$$

Let

$$z = (x+y^{2^i+1})^{\frac{1}{2^i+1}}.$$

Then according to equation (5), we have

$$(x+a+(y+b)^{2^i+1})^{\frac{1}{2^i+1}} = (x+y^{2^i+1})^{\frac{1}{2^i+1}} + b + d = z + b + d. \quad (6)$$

Raise both sides to the (2^i+1)th power, then we have

$$by^{2^i} + b^{2^i}y + (b+d)^{2^i}z + (b+d)z^{2^i} = a + b^{2^i+1} + (b+d)^{2^i+1}.$$

Furthermore, according to equality (6), it also holds

$$\begin{aligned} F^{'}(x,y) + F^{'}(x+a,y+b) &= y^{2^i}z + yz^{2^i} + (y+b)^{2^i}(z+b+d) + (y+b)(z+b+d)^{2^i} \\ &= (b+d)y^{2^i} + (b+d)^{2^i}y + b^{2^i}z + bz^{2^i} + b^{2^i}d + bd^{2^i}. \end{aligned}$$

Thus equation (4) implies

$$dy^{2^i} + d^{2^i}y + bz^{2^i} + b^{2^i}z = b^{2^i+1} + b^{2^i}d + bd^{2^i} + c.$$

Therefore, (x_0, y_0) is a root of equation

$$F(x,y) + F(x+a,y+b) = (c,d)$$

if and only if (y_0, z_0), where $z_0 = (x_0 + y_0^{2^i+1})^{\frac{1}{2^i+1}}$, is a root of the following system of equations

$$\begin{cases} dy^{2^i} + d^{2^i}y + bz^{2^i} + b^{2^i}z = b^{2^i+1} + b^{2^i}d + bd^{2^i} + c, \\ by^{2^i} + b^{2^i}y + (b+d)^{2^i}z + (b+d)z^{2^i} = a + b^{2^i+1} + (b+d)^{2^i+1}. \end{cases}$$

Notice that $(a,b) \neq (0,0)$, then $a \neq 0$ when $b = 0$. Note that $x^{\frac{1}{2^i+1}}$ is a permutation over $\mathbb{F}_{2^k}$, then (5) does not has solutions on $\mathbb{F}_{2^k}^2$ when $(b,d) = (0,0)$. Therefore, we have $(b,d) \neq (0,0)$ when the system of equation (4) and equation (5) has solutions in $\mathbb{F}_{2^k}^2$.

Hence according to Lemma 2, the above system of equations has 0 or 4 root in $\mathbb{F}_{2^k}^2$. Then we complete the proof. □

Theorem 5. *Suppose k is odd and $\gcd(i,k)=1$. Let $F(x,y)$ be the S-box over $\mathbb{F}_{2^k}^2$ constructed by three-round Feistel structure with round functions $P_1(x)=P_3(x)=x^{2^i+1}$ and $P_2(x)=x^{\frac{1}{2^i+1}}$. Then the nonlinearity of $F(x,y)$ equals $2^{2k-1}-2^k$, which is the best known nonlinearity over $\mathbb{F}_{2^k}^2$. Furthermore, the Walsh spectrum of $F(x,y)$ is $\{0,\pm 2^{k+1}\}$.*

Proof. Let $a,b,c,d\in\mathbb{F}_{2^k}$, and $(c,d)\neq(0,0)$. Then we have

$$\begin{aligned}&\lambda_F((a,b),(c,d))\\ =&\sum_{x,y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}(c(y^{2^i+1}+y^{2^i}(x+y^{2^i+1})^{\frac{1}{2^i+1}}+y(x+y^{2^i+1})^{\frac{2^i}{2^i+1}})+d(y+(x+y^{2^i+1})^{\frac{1}{2^i+1}})+ax+by)}.\end{aligned}$$

Let $z=(x+y^{2^i+1})^{\frac{1}{2^i+1}}$. Then $x=y^{2^i+1}+z^{2^i+1}$ and z runs over $\mathbb{F}_{2^k}$ when x runs over $\mathbb{F}_{2^k}$. Therefore, we have

$$\begin{aligned}\lambda_F((a,b),(c,d))&=\sum_{y,z\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}(c(y^{2^i+1}+y^{2^i}z+yz^{2^i})+d(y+z)+a(y^{2^i+1}+z^{2^i+1})+by)}\\&=\sum_{y,z\in\mathbb{F}_{2^k}}(-1)^{f(y,z)},\end{aligned}$$

where

$$f(y,z)=\mathrm{Tr}((a+c)y^{2^i+1}+az^{2^i+1}+c(y^{2^i}z+yz^{2^i})+(b+d)y+dz).$$

Firstly, if $a=c=0$, then $d\neq 0$ since $(c,d)\neq(0,0)$. Hence it holds

$$\begin{aligned}\lambda_F((0,b),(0,d))&=\sum_{y,z\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}((b+d)y+dz)}\\&=\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}((b+d)y)}\sum_{z\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}(dz)}\\&=0.\end{aligned}$$

Next, we suppose $(a,c)\neq(0,0)$. Note that

$$\begin{aligned}&f(y,z)+f(y+u,z+v)\\=&\mathrm{Tr}((a+c)(y^{2^i+1}+(y+u)^{2^i+1})+a(z^{2^i+1}+(z+v)^{2^i+1}))\\&+\mathrm{Tr}(c(y^{2^i}z+yz^{2^i}+(y+u)^{2^i}(z+v)+(y+u)(z+v)^{2^i})+(b+d)u+dv)\\=&\mathrm{Tr}((a+c)(u^{2^i}y+uy^{2^i}+u^{2^i+1})+a(v^{2^i}z+vz^{2^i}+v^{2^i+1}))\\&+\mathrm{Tr}(c(y^{2^i}v+u^{2^i}z+u^{2^i}v+yv^{2^i}+uz^{2^i}+uv^{2^i})+(b+d)u+dv)\\=&\mathrm{Tr}(((a+c)u^{2^i}+(au+cu)^{2^{n-i}}+cv^{2^i}+(cv)^{2^{n-i}})y)\\&+\mathrm{Tr}((av^{2^i}+(av)^{2^{n-i}}+cu^{2^i}+(cu)^{2^{n-i}})z)+f(u,v),\end{aligned}$$

then it holds that

$$\begin{aligned}\lambda_F((a,b),(c,d))^2 &= \sum_{y,z\in\mathbb{F}_{2^k}} (-1)^{f(y,z)} \times \sum_{u,v\in\mathbb{F}_{2^k}} (-1)^{f(y+u,z+v)} \\ &= \sum_{y,z,u,v\in\mathbb{F}_{2^k}} (-1)^{f(y,z)+f(y+u,z+v)} \\ &= \sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}((cv^{2^i}+(cv)^{2^{n-i}}+(a+c)u^{2^i}+(au+cu)^{2^{n-i}})y)} \\ &\quad \times \sum_{z\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}((cu^{2^i}+(cu)^{2^{n-i}}+av^{2^i}+(av)^{2^{n-i}})z)} \\ &\quad \times \sum_{u,v\in\mathbb{F}_{2^k}} (-1)^{f(u,v)} \\ &= 2^{2k} \sum_{u,v\in R(a,c)} (-1)^{f(u,v)},\end{aligned}$$

where $R(a,c)$ is the solution set of the following system of equations with variables u and v

$$\begin{cases} av^{2^i} + (av)^{2^{n-i}} + cu^{2^i} + (cu)^{2^{n-i}} = 0, \\ cv^{2^i} + (cv)^{2^{n-i}} + (a+c)u^{2^i} + (au+cu)^{2^{n-i}} = 0. \end{cases}$$

Note that $(a,c) \neq (0,0)$, then according to Lemma 3, the above system of equations has exactly 4 roots in $\mathbb{F}_{2^k}^2$. Denote

$$R(a,c) = \{(u_i, v_i) \mid 0 \leq i \leq 3\}.$$

Notice that $f(y,z)+f(y+u,z+v) = f(u,v)$ for $(u,v) \in R(a,c)$ and $(y,z) \in \mathbb{F}_{2^k}^2$, which means $f(u,v)$ is linear on $R(a,c)$. Therefore, $f(u,v)$ is a balanced function or a constant 0 on $R(a,c)$. Note that $(0,0) \in R(a,c)$, then it holds

$$\lambda_F((a,b),(c,d))^2 = \begin{cases} 2^{2k+2} & f(u_i,v_i) = 0 \text{ for all } 0 \leq i \leq 3, \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\lambda_F((a,b),(c,d)) \in \{0, \pm 2^{k+1}\},$$

and we complete the proof. □

At the end of this section, we investigate the algebraic degree of $F(x,y)$. The following results are needed.

Lemma 4. *[22] Suppose k is odd and $gcd(i,k) = 1$. Then the compositional inverse of x^{2^i+1} over $\mathbb{F}_{2^k}$ is x^t, where $t = \sum_{j=0}^{\frac{k-1}{2}} 2^{2ij} \bmod (2^k-1)$. Its algebraic degree is $\frac{k+1}{2}$.*

Lemma 5. *[4,7] Suppose $F(x) \in \mathbb{F}_{2^n}[x]$. If $\lambda_F(a,b) \in \{0, \pm 2^{\frac{n+s}{2}}\}$ for all $b \in \mathbb{F}_{2^n}^*$ and $a \in \mathbb{F}_{2^n}$, then $d^\circ(F) \leq \frac{n-s}{2} + 1$.*

Theorem 6. *Suppose k is odd and $\gcd(i,k) = 1$. Let $F(x,y)$ be the S-box over $\mathbb{F}_{2^k}^2$ constructed by three-round Feistel structure with round functions $P_1(x) = P_3(x) = x^{2^i+1}$ and $P_2(x) = x^{\frac{1}{2^i+1}}$. Then the algebraic degree of $F(x,y)$ equals k.*

Proof. Firstly, according to Theorem 5 and Lemma 5, we have

$$d^\circ(F(x,y)) \leq \frac{2k-2}{2} + 1 = k.$$

Next, let $S = \{2ij \bmod k \mid 0 \leq j \leq \frac{k-1}{2}\}$ and for $s \subseteq S$, define

$$2^s = \begin{cases} 0 & s = \emptyset, \\ \sum\limits_{j \in s} 2^j \bmod (2^k - 1) & s \neq \emptyset. \end{cases}$$

Then according to Lemma 4, the compositional inverse of x^{2^i+1} is x^{2^S}. Hence we have

$$\begin{aligned}
(x + y^{2^i+1})^{\frac{1}{2^i+1}} &= (x + y^{2^i+1})^{2^S} \\
&= \sum_{s_1 \subseteq S} x^{2^{s_1}} y^{(2^i+1)2^{S \setminus s_1}} \\
&= xy^{(2^i+1)\sum\limits_{j=1}^{\frac{k-1}{2}} 2^{2ji} \bmod (2^k-1)} + \sum_{\{0\} \neq s_1 \subseteq S} x^{2^{s_1}} y^{(2^i+1)2^{S \setminus s_1}} \\
&= xy^{d_1} + F'(x,y),
\end{aligned}$$

where $F'(x,y) = \sum\limits_{\{0\} \neq s_1 \subseteq S} x^{2^{s_1}} y^{(2^i+1)2^{S \setminus s_1}}$ and

$$d_1 = (2^i+1)\sum_{j=1}^{\frac{k-1}{2}} 2^{2ji} \bmod (2^k-1) = \sum_{j=2}^{k} 2^{ji} \bmod (2^k-1).$$

We claim that $\omega_2(d_1) = k-1$. Otherwise there exist $2 \leq j_1 < j_2 \leq k$, such that $2^{ij_1} = 2^{ij_2} \bmod (2^k-1)$. This is equivalent to $ij_1 = ij_2 \bmod k$, since for an integer $r \in \mathbb{Z}$, $2^r \bmod (2^k-1) = 2^{r'}$, where $0 \leq r' \leq k-1$ and $r' = r \bmod k$. Thus $k | i(j_2 - j_1)$. Note that $\gcd(i,k) = 1$, then $j_1 = j_2$, which is a contradiction. Therefore, it holds

$$\omega_2(d_1) = k-1,$$

and hence

$$d^\circ(xy^{d_1}) = k.$$

Notice that xy^{d_1} does not appear in the terms of $F'(x,y)$, then the algebraic degree of $y + (x + y^{2^i+1})^{\frac{1}{2^i+1}}$ equals k. This means $F(x,y)$ has a component function with algebraic degree k. Thus $d^\circ(F(x,y)) \geq k$. Then we complete the proof. □

According to the above results, we have the following result.

Theorem 7. *Suppose k is an odd integer and* $\gcd(i,k)=1$. *Let*

$$F(x,y)=(x+y^{2^i+1}+(y+(x+y^{2^i+1})^{\frac{1}{2^i+1}})^{2^i+1},y+(x+y^{2^i+1})^{\frac{1}{2^i+1}}),$$

which is the S-box over $\mathbb{F}_{2^k}^2$ constructed by three-round Feistel structure with round functions $P_1=P_3=(x)^{2^i+1}$ and $P_2=P_1(x)^{-1}=x^{\frac{1}{2^i+1}}$. Then the following statements hold.

(1) $F(x,y)$ is an involution over $\mathbb{F}_{2^k}^2$, which means $F(F(x,y))=(x,y)$.
(2) The differential uniformity of $F(x,y)$ equals 4 and its differential spectrum is $\{0,4\}$.
(3) The nonlinearity of $F(x,y)$ equals $2^{2k-1}-2^k$ and its Walsh spectrum is $\{0,\pm 2^{k+1}\}$.
(4) The algebraic degree of $F(x,y)$ equals k.

Remark 1. When $k=3$, $i=1$, it can be checked that $F(x,y)$ in Theorem 7 is CCZ-equivalent to x^5. In general, we do not know whether $F(x,y)$ is CCZ-equivalent to the Gold type permutations over $\mathbb{F}_{2^{2k}}$, i.e., x^{2^i+1} with $\gcd(i,2k)=2$. However, the permutations in Theorem 7 are still interesting due to their efficient hardware implementation.

The following result also holds, whose proof is similar to the proof of above results.

Theorem 8. *Suppose k is an odd integer and* $\gcd(i,k)=1$, $\alpha,\beta,\gamma\in\mathbb{F}_{2^k}$. *Let*

$$F(x,y)=(x+(y+\alpha)^{2^i+1}+(y+\gamma+(x+\beta+(y+\alpha)^{2^i+1})^{\frac{1}{2^i+1}})^{2^i+1},y+(x+\beta+(y+\alpha)^{2^i+1})^{\frac{1}{2^i+1}}),$$

which is the S-box over $\mathbb{F}_{2^k}^2$ constructed by three-round Feistel structure with round functions $P_1(x)=(x+\alpha)^{2^i+1}$, $P_2(x)=(x+\beta)^{\frac{1}{2^i+1}}$ and $P_3(x)=(x+\gamma)^{2^i+1}$. Then the following statements hold.

(1) $F(x,y)$ is an involution over $\mathbb{F}_{2^k}^2$ when $\alpha=\gamma$.
(2) The differential uniformity of $F(x,y)$ equals 4 and its differential spectrum is $\{0,4\}$.
(3) The nonlinearity of $F(x,y)$ equals $2^{2k-1}-2^k$ and its Walsh spectrum is $\{0,\pm 2^{k+1}\}$.
(4) The algebraic degree of $F(x,y)$ equals k.

Remark 2. "Characterizing the F-functions whose maximum differential probability with keys is small" is an open problem proposed in [1]. In that paper, the i-th round of Feistel structure is a transformation as $(L_i,R_i)\rightarrow(R_i,L_i+f(L_i+k_i))$. F-function means $f(x+k_i)$, where f is a permutation and k_i is the i-th round key. Theorem 8 means that for any fixed round keys, the three-round Feistel scheme with round functions $P_1=P_3=x^{2^i+1}$ and $P_2=x^{\frac{1}{2^i+1}}$ always posses the best differential uniformity and nonlinearity.

5 Constructing Optimal 4-bit S-boxes with Unbalanced Feistel Structure

Four bit S-boxes are always chosen for lightweight cryptography because of their less hardware implementation cost. It has been shown that, the best differential uniformity and nonlinearity of 4-bit S-boxes both equal 4 [17]. These S-boxes are called optimal 4-bit S-boxes.

In order to reduce hardware implementation cost, a method of constructing recursive diffusion layers is proposed in PHONTON [14] and LED [15], and further studied in [26]. We use a similar idea to construct recursive S-boxes in this section. We show that some optimal 4-bit S-boxes can be constructed with 4 or 5 round unbalanced Feistel structure.

Construction 1. *Suppose f is a nonlinear Boolean function with three variables, and $x_i \in \mathbb{F}_2, 1 \leq i \leq 4$. One round unbalanced Feistel structure is a transformation as follows*

$$P_f(x_1, x_2, x_3, x_4) = (x_2, x_3, x_4, x_1 + f(x_2, x_3, x_4)).$$

Then an S-box over $\mathbb{F}_2^4$ can be constructed with t round unbalanced Feistel structure as follows

$$F(x_1, x_2, x_3, x_4) = P_f^t(x_1, x_2, x_3, x_4),$$

where $t = 4$ or 5, P_f^j defined as $P_f(P_f^{j-1})$ for $j \geq 2$ and $P_f^1 = P_f$.

It is easy to see that P_f^t is a permutation over $\mathbb{F}_2^4$ for $t \geq 1$. In order to update every bit of the output of the S-boxes constructed as above, t should larger than or equal to 4. Considering the efficiency of S-boxes, it is better to construct S-boxes with not too many rounds. Thus, we choose $t = 4$ or 5 in the above construction. P_f^t can be implemented with nonlinear feedback register (NLFSR) as shown in Figure 2. It also can be implemented similarly as the implementation of S-boxes in Piccolo [23] and LS-design [13].

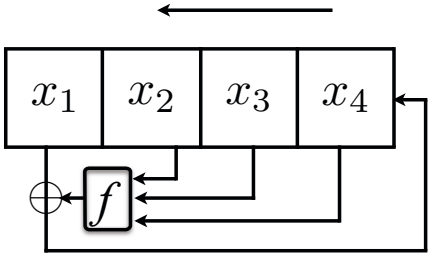

Fig. 2. Constructing S-box with NLFSR

Table 2. Boolean functions such that P_f^4 are optimal 4-bit S-boxes

f	Operations	G_i	f	Operations	G_i
x_2x_3	(1, 1, 0)	8	x_2x_3+1	(1, 1, 1)	8
x_3x_4	(1, 1, 0)	8	x_3x_4+1	(1, 1, 1)	8
$(x_3+1)x_4$	(1, 1, 1)	8	$(x_3+1)x_4+1^\star$	(1, 1, 2)	8
$x_2(x_3+1)$	(1, 1, 1)	8	$x_2(x_3+1)+1^\star$	(1, 1, 2)	8
$x_3(x_4+1)$	(1, 1, 1)	8	$x_3(x_4+1)+1^\star$	(1, 1, 2)	8
$(x_2+1)x_3$	(1, 1, 1)	8	$(x_2+1)x_3+1^\star$	(1, 1, 2)	8
$(x_2+1)(x_3+1)+1$	(1, 1, 3)	8	$(x_2+1)(x_3+1)$	(1, 1, 2)	8
$(x_3+1)(x_4+1)+1$	(1, 1, 3)	8	$(x_3+1)(x_4+1)$	(1, 1, 2)	8
$x_2x_3+x_4$	(2, 1, 0)	8	$x_2x_3+x_4+1^\star$	(2, 1, 1)	8
$x_2+x_3x_4$	(2, 1, 0)	8	$x_2+x_3x_4+1^\star$	(2, 1, 1)	8
$x_2+(x_3+1)x_4$	(2, 1, 1)	8	$x_2+(x_3+1)x_4+1$	(2, 1, 2)	8
$(x_2+1)x_3+x_4$	(2, 1, 1)	8	$(x_2+1)x_3+x_4+1$	(2, 1, 2)	8
$x_2+x_3(x_4+1)$	(2, 1, 1)	8	$x_2+x_3(x_4+1)+1$	(2, 1, 2)	8
$x_2(x_3+1)+x_4$	(2, 1, 1)	8	$x_2(x_3+1)+x_4+1$	(2, 1, 2)	8
$x_2+(x_3+1)(x_4+1)+1$	(2, 1, 3)	8	$x_2+(x_3+1)(x_4+1)^\star$	(2, 1, 2)	8
$(x_2+1)(x_3+1)+x_4+1$	(2, 1, 3)	8	$(x_2+1)(x_3+1)+x_4^\star$	(2, 1, 2)	8
$x_2(x_3+x_4)+x_3x_4$	(3, 2, 0)	1	$x_2(x_3+x_4)+x_3x_4+1$	(3, 2, 1)	1
$x_2(x_4+x_3+1)+(x_3+1)x_4$	(3, 2, 1)	1	$x_2(x_4+x_3+1)+(x_3+1)x_4+1$	(3, 2, 2)	1
$x_2(x_3+x_4+1)+x_3(x_4+1)$	(3, 2, 1)	1	$x_2(x_3+x_4+1)+x_3(x_4+1)+1$	(3, 2, 2)	1
$(x_2+1+x_4)x_3+(x_2+1)x_4$	(3, 2, 1)	1	$(x_2+1+x_4)x_3+(x_2+1)x_4+1$	(3, 2, 2)	1

Let $Q_f(x_1,x_2,x_3,x_4)=(x_4+f(x_1,x_2,x_3),x_1,x_2,x_3)$, which is also a transformation that can be implemented easily. Then it is easy to verify that

$$P(Q(x_1,x_2,x_3,x_4))=(x_1,x_2,x_3,x_4).$$

Hence the compositional inverse of P_f^t equals Q_f^t. It should be noticed Q_f^t also can be implemented with nonlinear shift register.

By an exhaustive searching, we list all Boolean functions f such that P_f^4, P_f^5 are optimal 4-bit S-boxes in Table 2 and Table 3 respectively. The cost of hardware implementation of one round transformations of P_f^t, i.e. x_1+f, is estimated in the two tables. An element "(r_1,r_2,r_3)" in the "Operations" columns of the two tables means that the number of operations "+" (XOR), "$*$" (AND) and "+1" (NOT) in x_1+f is r_1, r_2 and r_3 respectively.

According to [17], there are exactly 16 classes of optimal 4-bit S-boxes up to affine equivalence. An element "j" in the columns "G_i" in Table 2 (resp. Table 3) means the P_f^4 (resp. P_f^5) is CCZ-equivalent to G_j in [17]. It can be checked that the S-box used in PRESENT [2] is affine equivalent to G_1.

The functions with a "$\star$" in the superscript, such as "$f^\star$", in Table 2 (resp. Table 3) means that P_f^4 (resp. P_f^5) does not have fixed points. For other functions in the two tables, it can be checked that there always exists nonzero constant $(a_1,a_2,a_3,a_4)\in\mathbb{F}_2^4$, such that $P_f^4(x_1+a_1,x_2+a_2,x_3+a_3,x_4+a_4)$ (resp. $P_f^5(x_1+a_1,x_2+a_2,x_3+a_3,x_4+a_4)$) does not have fixed points. Note that adding a constant to input does not change the differential uniformity and nonlinearity, then for any function f in the two tables, optimal 4-bit S-boxes with no fixed

Table 3. Boolean functions such that P_f^5 are optimal 4-bit S-boxes

f	Operations	G_i	f	Operations	G_i
$x_2(x_3+x_4)+1$	(2, 1, 1)	7	$(x_2+x_4)x_3+1^\star$	(2, 1, 1)	4
$(x_2+x_3)x_4+1$	(2, 1, 1)	7	$(x_2+x_4)(x_3+1)+1^\star$	(2, 1, 2)	4
$(x_2+x_3)(x_4+1)+1$	(2, 1, 2)	7	$(x_2+1)(x_3+x_4)+1$	(2, 1, 2)	7
$x_2x_3+(x_2+1)x_4$	(2, 2, 1)	13	$x_2(x_4+1)+x_3x_4$	(2, 2, 1)	13
$x_2x_4+x_3(x_4+1)+1$	(2, 2, 2)	13	$x_2(x_3+1)+x_3(x_4+1)$	(2, 2, 2)	4
$(x_2+1)x_3+x_2x_4+1$	(2, 2, 2)	13	$x_2x_4+(x_3+1)(x_4+1)^\star$	(2, 2, 2)	13
$x_2x_3+(x_2+1)(x_4+1)^\star$	(2, 2, 2)	13	$(x_2+1)(x_4+1)+x_3x_4^\star$	(2, 2, 2)	13
$(x_2+1)(x_3+1)+x_2x_4^\star$	(2, 2, 2)	13	$(x_2+1)x_3+(x_3+1)x_4$	(2, 2, 2)	4
$x_2((x_3+1)x_4+1)+x_3(x_4+1)$	(2, 3, 3)	11	$(x_2(x_4+1)+1)x_3+(x_2+1)x_4$	(2, 3, 3)	11
$(x_2x_3+1)x_4+(x_2+1)(x_3+1)$	(2, 3, 3)	11	$x_2(x_3x_4+1)+(x_3+1)(x_4+1)$	(2, 3, 3)	11
$(x_2x_3+1)x_4+(x_2+1)(x_3+1)+1$	(2, 3, 4)	11	$(x_2x_4+1)x_3+(x_2+1)(x_4+1)+1$	(2, 3, 4)	3
$x_2(x_3x_4+1)+(x_3+1)(x_4+1)+1$	(2, 3, 4)	11	$x_2(x_3(x_4+1)+1)+(x_3+1)x_4+1$	(2, 3, 4)	3
$(x_2(x_4+1)+1)x_3+(x_2+1)x_4+1$	(2, 3, 4)	11	$x_2((x_3+1)x_4+1)+x_3(x_4+1)+1$	(2, 3, 4)	11

points can also be constructed by adding a constant to the input. For example, let $f = x_2x_3$, by adding $(1, 0, 1, 0)$ to the input of P_f^4, we have $P_f^4(x_1+1, x_2, x_3+1, x_4)$ is a optimal 4-bit S-boxes which does not have fixed points.

With the method in this section, it can only use 1 XOR, 1 AND and 2 NOT for one round transformation to construct an 4-bit optimal S-box with no fixed points by 4 round unbalanced Feistel structure, see Table 2.

6 Conclusion

In the present paper, we investigate cryptographic properties of S-boxes constructed with three-round Feistel structure. A class of differential 4-uniform S-boxes with the best known nonlinearity over $\mathbb{F}_{2^k}^2$ for k odd is given. It is also shown that optimal 4-bit S-boxes can be constructed with unbalanced Feistel structure and some experiment results are given in the paper. The problem of constructing new, which means CCZ-inequivalent to known ones, differential 4-uniform permutations over $\mathbb{F}_{2^k}^2$ with the best known nonlinearity is an interesting problem that needs further study.

Acknowledgements. We are grateful to the anonymous reviewers for their valuable comments on this paper which have improved the presentation of the paper greatly. This work was supported by the 973 project under Grant (2013CB834203), by the National Science Foundation of China (No.61303255, No.61379142).

References

1. Aoki, K.: On maximum non-averaged differential probability. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, pp. 118–130. Springer, Heidelberg (1999)

2. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
3. Budaghyan, L., Carlet, C., Pott, A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. on Inform. Theory 52(3), 1141–1152 (2006)
4. Budaghyan, L., Pott, A.: On differential uniformity and nonlinearity of functions. Discrete Mathematics 309(2), 371–384 (2009)
5. Canright, D.: A Very Compact S-Box for AES. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 441–455. Springer, Heidelberg (2005)
6. Canteaut, A.: Differential cryptanalysis of Feistel ciphers and differentially δ-uniform mappings. In: Workshop on Selected Areas in Cryptography (SAC 1997), pp. 172–184 (1997)
7. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations sutiable for DES-like cryptosystems. Des. Codes Cryptogr. 15(2), 125–156 (1998)
8. Carlet, C.: Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press (2010)
9. Carlet, C.: Vectorial Boolean Functions for Cryptography, Chapter of the monography. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Press (2010)
10. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 356–365. Springer, Heidelberg (1995)
11. Dobbertin, H.: One-to-one highly nonlinear power functions on $GF(2^n)$. Appl. Algebra Engrg. Comm. Comput. 9(2), 139–152 (1998)
12. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory 14, 154–156 (1968)
13. Grosso, V., Leurent, G., Standaert, F.-X., Varici, K.: LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations. In: FSE 2014 (2014)
14. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer, Heidelberg (2011)
15. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
16. Hou, X.D.: Affinity of permutations of $\mathbb{F}_2^n$. Discrete Appl. Math. 154(2), 313–325 (2006)
17. Leander, G., Poschmann, A.: On the Classification of 4 Bit S-Boxes. In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 159–176. Springer, Heidelberg (2007)
18. Lim, C.H.: CRYPTON: A new 128-bit block cipher. In: The First AES Candidate Conference. National Institute for Standards and Technology (1998)
19. Matsui, M.: New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 205–218. Springer, Heidelberg (1996)
20. Matsui, M.: New block encryption algorithm MISTY. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)

21. Nyberg, K., Knudsen, L.R.: Provable security against differential cryptanalysis. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 566–574. Springer, Heidelberg (1993)
22. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994)
23. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: *Piccolo*: An Ultra-Lightweight Blockcipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 342–357. Springer, Heidelberg (2011)
24. Stern, J., Vaudenay, S.: CS-CIPHER. In: Vaudenay, S. (ed.) FSE 1998. LNCS, vol. 1372, pp. 189–204. Springer, Heidelberg (1998)
25. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4: Design and Evaluation Report, version 1.3 (2011)
26. Wu, S., Wang, M., Wu, W.: Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 355–371. Springer, Heidelberg (2013)