Lai-Massey Scheme Revisited

M. R. Mirzaee Shamsabad[1] and S. M. Dehnavi[2]

[1] Faculty of Applied Mathematics, Shahid Beheshti University, Tehran, Iran,
m_mirzaee@sbu.ac.ir
[2] Department of Mathematical and Computer Sciences, University of Kharazmi, Tehran, Iran,
dehnavism@ipm.ir

Abstract. Lai-Massey scheme is a well-known block cipher structure which has been used in the design of the ciphers PES, IDEA, WIDEA, FOX and MESH. Recently, the lightweight block cipher FLY applied this structure in the construction of a lightweight 8×8 S-box from 4×4 ones. In the current paper, firstly we investigate the linear, differential and algebraic properties of the general form of the S-boxes used in FLY, mathematically. Then, based on this study, a new cipher structure is proposed which we call generalized Lai-Massey scheme or GLM. We give upper bounds for the maximum average differential probability (MADP) and maximum average linear hull (MALH) of GLM and after examination of impossible differentials and zero-correlations of one round of this structure, we show that two rounds of GLM do not have any structural impossible differentials or zero-correlations. As a measure of structural security, we prove the pseudo-randomness of GLM by the H-coefficient method.
Keywords: Generalized Lai-Massey Scheme; S-box; Symmetric Cipher; H-coefficient method; MADP; MALH.

1 Introduction

Feistel scheme is a well-known and widely used structure in symmetric cryptography. Many block ciphers are designed by this scheme; among them are DES [2], FEAL [9], SKIPJACK [12], KASUMI [5] and SIMON [1]. Feistel scheme is also used for construction of S-boxes of the symmetric ciphers CS [13], CRYPTON [7] and ZUC [14]. For another example, the FI function of the block cipher MISTY [8] is based upon the Feistel scheme.
The Lai-Massey scheme was used for the first time in 1990 in the design of PES (Proposed Encryption Standard) [6] by Lai and Massey. After the advent of linear and differential cryptanalysis, a modified cipher IDEA (International Data Encryption Algorithm) was designed by Lai, Massey and Murphy in 1991. Among other ciphers designed after Lai-Massey scheme are WIDEA, FOX [3] and MESH [11] families of block ciphers. Recently, the designers of the lightweight block cipher FLY [4] have used a modified version of Lai-Massey structure in the design of its S-box Littlun.
In this paper, firstly we examine the cryptographic properties of the general

form of the S-boxes constructed in the FLY block cipher. More precisely, we give bounds for maximum differential uniformity and linearity of these kinds of S-boxes, for some cases. Also, in some spacial cases, we give the algebraic degree of the mentioned S-boxes.
Then, we propose a new structure for symmetric ciphers which we call generalized Lai-Massey scheme or GLM for short, and present lower bounds for maximum average differential probability (MADP) and maximum average linear hull (MALH) of one round of this structure. Also, we study impossible differentials and zero-correlations of one and two rounds of GLM. We show that, two rounds of GLM do not have any structural impossible differentials or zero-correlations. We prove the pseudo-randomness of the proposed structure by the H-coefficient method, as a measure of structural security.
According to the upper bounds for MADP and MALH, GLM is comparable to three rounds of a classic 2-branch Feistel scheme. An advantage of the proposed scheme over the Feistel structure is that, the first layer in the construction of GLM could be implemented in parallel, which could render it faster in software and hardware implementations.
In Section 2, we give the preliminaries for the rest of the paper. Section 3 is devoted to the theoretical examinations of the paper. Section 4 is the conclusion.

2 Preliminaries

The finite field with 2^n elements is denoted by $\mathbb{F}_{2^n}$ and the n-dimensional linear space over $\mathbb{F}_2$ is represented by $\mathbb{F}_2^n$. For a map f on $\mathbb{F}_{2^n}$, it can be shown that f has a representation (unique up to the choice of the representing irreducible polynomial)

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

where $a_i \in \mathbb{F}_{2^n}$, $0 \leq i < 2^n$. The algebraic degree of f is defined as

$$deg(f) = \max_{0 \leq i < 2^n, a_i \neq 0} wt(i).$$

Here, $wt(i)$ means the Hamming weight of i. Also, for a map f on $\mathbb{F}_{2^{2n}}$, it is proved that f has a representation (unique up to the choice of the representing irreducible polynomial)

$$f(x, y) = \sum_{0 \leq i,j < 2^n} a_{i,j} x^i y^j,$$

where $a_{i,j} \in \mathbb{F}_{2^n}$, $0 \leq i, j < 2^n$. The algebraic degree of f is also defined as

$$deg(f) = \max_{0 \leq i,j < 2^n, a_{i,j} \neq 0} (wt(i) + wt(j)).$$

These two notions of algebraic degree coincide with each other.
Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. For any $a \neq 0, b \in \mathbb{F}_{2^n}$, set

$$D_f(a, b) = \{x \in \mathbb{F}_{2^n} : f(x) \oplus f(x \oplus a) = b\}.$$

Here, $\oplus$ stands for the XOR operation. The maximum differential uniformity of f is defined as

$$\Delta_f = max_{a\neq 0,b} D_f(a,b).$$

The table $D_f(a,b)$ for $a,b \in \mathbb{F}_2^n$ is called the differential distribution table (DDT) of f. Also, for any $a,b \neq 0 \in \mathbb{F}_{2^n}$, define

$$L_f(a,b) = \sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x \oplus b\cdot f(x)}.$$

Here, $\cdot$ stands for the standard dot product in $\mathbb{F}_2^n$, which is viewed as an n-dimensional linear space over $\mathbb{F}_2$. The linearity of f is defined as

$$\Lambda_f = max_{a,b\neq 0} |L_f(a,b)|.$$

The table $L_f(a,b)$ for $a,b \in \mathbb{F}_2^n$ is called the linear approximation table (LAT) of f.
Let $y = F(x,K)$ with $x,y \in \mathbb{F}_2^n$ and $K \in \mathbb{F}_2^m$ be a (keyed) mapping. For given differentials $\Delta x, \Delta y \in \mathbb{F}_2^n$, the average differential probability of F on $(\Delta x, \Delta y)$ is

$$DP_F(\Delta x, \Delta y) = \frac{1}{2^m} \sum_{K\in\mathbb{F}_2^m} P_x\{F(x\oplus\Delta x, K) \oplus F(x,K) = \Delta y\}.$$

The MADP of F is defined as

$$DP(F) = max_{\Delta x\neq 0,\Delta y} DP_F(\Delta x, \Delta y).$$

For given masks $\Gamma_x, \Gamma_y \in \mathbb{F}_2^n$, the average linear hull of F on (Γ_x, Γ_y) is

$$LH_F(\Gamma_x, \Gamma_y) = \frac{1}{2^m} \sum_{K\in\mathbb{F}_2^m} |2P_x\{x\cdot\Gamma_x = F(x,K)\cdot\Gamma_y\} - 1|^2.$$

The MALH of F is defined as

$$LH(F) = max_{\Gamma_x,\Gamma_y\neq 0} LH_F(\Gamma_x, \Gamma_y).$$

3 Generalized Lai-Massey Scheme (GLM)

In this section, firstly we investigate the general form of S-boxes presented in the FLY block cipher and give bounds on their maximum differential uniformities as well as their linearities, in some cases. We compute their algebraic degrees in some special cases. Then, we propose GLM and give lower bounds on MADP as well as MALH of one round of this structure. We also investigate impossible diffrentials and zero-correlations of GLM. Finally, we prove the pseudo-randomness of the proposed structure.

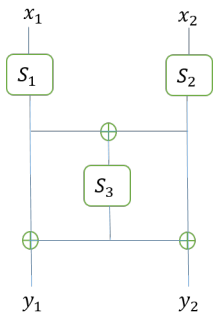

Fig. 1.

3.1 General form of the S-boxes in FLY

In this subsection, we investigate S-boxes which are constructed based on the structure of the S-boxes of FLY [4]. Figure 1 is the general form of the Littlun S-box of the FLY block cipher. Suppose that S_1, S_2 and S_3 are three $n \times n$ S-boxes (maps on $\mathbb{F}_2^n$) such that S_1 and S_2 are bijective. We have:

$$S(y_1, y_2) = (S_1(x_1) \oplus S_3(S_1(x_1) \oplus S_2(x_2)), S_2(x_2) \oplus S_3(S_1(x_1) \oplus S_2(x_2))). \quad (1)$$

Figure 2 depicts the inverse of this S-box. The direct formula for its inverse is:

$$S^{-1}(x_1, x_2) = (S_1^{-1}(y_1 \oplus S_3(y_1 \oplus y_2)), S_2^{-1}(y_2 \oplus S_3(y_1 \oplus y_2))).$$

In the next lemma, we give a bound for maximum differential uniformity of the proposed structure, in some cases.

Lemma 1. *Suppose that the maximum differential uniformity of S_1, S_2, S_3 and S are Δ_1, Δ_2, Δ_3 and Δ, respectively. Suppose that the following property holds for S_1 and S_3: there are $a, b \in \mathbb{F}_2^n$ such that $D_{S_1}(a, b) = \Delta_1$ and $D_{S_3}(b, a) = \Delta_3$, and a similar property holds for S_2 and S_3. Then, we have*

$$\Delta \geq \max\{\Delta_1\Delta_3, \Delta_2\Delta_3\}.$$

Proof. Put $\alpha = a$ and $\gamma = a \oplus b$. Consider

$$D_F((\alpha, 0), (\gamma, \alpha)) = \{(x_1, x_2) | S(x_1, x_2) \oplus S(x_1 \oplus \alpha, x_2) = (\gamma, \alpha)\},$$

or

$$\begin{cases} S_1(x) \oplus S_1(x_1 \oplus \alpha) = \gamma \oplus \alpha, \\ S_3(S_1(x_1) \oplus S_2(x_2)) \oplus S_3(S_1(x_1 \oplus \alpha) \oplus S_2(x_2)) = \alpha. \end{cases}$$

Now, considering the first equation, we have $x_1 \in D_{S_1}(\alpha, \gamma \oplus \alpha)$. So, we have

$$(S_1(x_1) \oplus S_2(x_2)) \oplus (S_1(x_1 \oplus \alpha) \oplus S_2(x_2)) = S_1(x_1) \oplus S_1(x_1 \oplus \alpha) = \gamma \oplus \alpha.$$

Put $z = S_1(x_1) \oplus S_2(x_2)$. *We have*

$$S_3(z) \oplus S_3(z \oplus (\gamma \oplus \alpha)) = \alpha,$$

which means that

$$x_2 \in S_2^{-1}(S_1(x_1) \oplus D_{S_3}(\gamma \oplus \delta, \alpha)).$$

Since

$$\Delta \geq D_S((\alpha, 0), (\gamma, \alpha)),$$

so, we have

$$\Delta \geq \{\Delta_1 \Delta_3\}.$$

Similarly, we have

$$\Delta \geq \{\Delta_2 \Delta_3\}.$$

Thus,

$$\Delta \geq \max\{\Delta_1 \Delta_3, \Delta_2 \Delta_3\}.$$

□

Remark 1. In the following three cases, the conditions of Lemma 1 are satisfied and we have:
a) If $S_3 = S_1^{-1}$, then $\Delta \geq \max\{\Delta_1^2, \Delta_2 \Delta_3\}$.
b) If $S_3 = S_2^{-1}$, then $\Delta \geq \max\{\Delta_2^2, \Delta_1 \Delta_3\}$.
c) If $S_1 = S_2$ and $S_3 = S_1^{-1}$, then $\Delta \geq \Delta_1^2$.

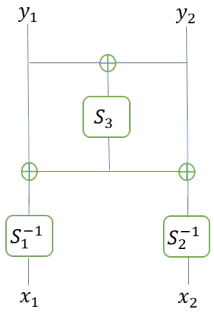

Fig. 2.

In the next lemma, we give a bound on the linearity of the proposed structure, in some cases.

Lemma 2. *Let the linearities of* S_1, S_2, S_3 *and* S *be* Λ_1, Λ_2, Λ_3 *and* Λ, *respectively. Suppose that the following criterion holds for* S_1 *and* S_3*: there are* $a, b \in \mathbb{F}_2^n$ *such that* $L_{S_1}(a, b) = \Lambda_1$ *and* $L_{S_3}(a, b) = \Lambda_3$. *Further, a similar criterion holds for* S_2 *and* S_3. *Then*

$$\Lambda \geq max\{\Lambda_1 \Lambda_3, \Lambda_2 \Lambda_3\}.$$

Proof. Supposing that $a = \alpha$ *and* $\gamma = a \oplus b$*, we have*

$$\begin{aligned}
|L_S((\alpha,0),(\gamma,\alpha))| &= |\sum_{(x,y)\in(\mathbb{F}_2^n)^2} (-1)^{(\alpha,0)\cdot(x,y)\oplus(\gamma,\alpha)\cdot S(x,y)}| \\
&= |\sum_{(x,y)\in(\mathbb{F}_2^n)^2} (-1)^{\alpha\cdot x\oplus\gamma\cdot S_1(x)\oplus\gamma\cdot S_3(z)\oplus\alpha\cdot S_2(y)\oplus\alpha\cdot S_3(z)}| \\
&= |\sum_{x\in\mathbb{F}_2^n}((-1)^{\alpha\cdot x\oplus(\alpha\oplus\gamma)\cdot S_1(x)} \sum_{y\in\mathbb{F}_2^n}(-1)^{\alpha\cdot z\oplus(\alpha\oplus\gamma)\cdot S_3(z)})| \\
&= |\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x\oplus(\alpha\oplus\gamma)\cdot S_1(x)}\Lambda_3| \\
&= \Lambda_3|\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x\oplus(\alpha\oplus\gamma)\cdot S_1(x)}| \\
&= \Lambda_1\Lambda_3,
\end{aligned}$$

where $z = S_1(x) \oplus S_2(y)$*. Now, since* $\Lambda \geq |L_S((\alpha,0),(\gamma,\alpha))|$*, so* $\Lambda \geq \Lambda_1\Lambda_3$*. Similarly,* $\Lambda \geq \Lambda_2\Lambda_3$*. So,*

$$\Lambda \geq max\{\Lambda_1\Lambda_3, \Lambda_2\Lambda_3\}.$$

□

Remark 2. In the case that $S_1 = S_2 = S_3$, the conditions of Lemma 2 are satisfied and we have $\Lambda \geq \Lambda_1^2$.

In the two following lemmas, we determine the algebraic degree of the proposed S-boxes in some special cases.

Lemma 3. *In the case that* $S_1(x) = S_2(x) = S_3(x) = x^{-1} = x^{2^n-2}$ *on* $\mathbb{F}_{2^n}$*, we have* $deg(S) \geq n+1$*.*

Proof. Consider the left output argument of (1). Note that for simplicity, we set $x_1 = x$ *and* $x_2 = y$*:*

$$\begin{aligned}
S_1(x) \oplus S_3(S_1(x) \oplus S_2(y)) &= x^{2^n-2} \oplus (x^{2^n-2} \oplus y^{2^n-2})^{2^n-2} \\
&= x^{2^n-2} \oplus (x^{2^n-2})^{2^n-2} \oplus (x^{2^n-2})^{2^n-4}(y^{2^n-2})^2 \oplus \cdots .
\end{aligned}$$

Here, we have used the well-known binomial expansion formula. Consider the monomial $(x^{2^n-2})^{2^n-4}(y^{2^n-2})^2$*. Since*

$$(2^n-2)(2^n-4) = 3 \mod (2^n-1),$$

$$2(2^n-2) = 2^n-3 \mod (2^n-1),$$

and

$$wt(3) = 2, \quad wt(2^n-3) = n-1,$$

we have $wt(3) + wt(2^n-3) = n+1$*; which means that* $deg(S) \geq n+1$*.* □

Lemma 4. *In the case that* $S_1(x) = S_2(x) = x^{-1}$ *and* $S_3(x) = x^3$ *on* $\mathbb{F}_{2^n}$*, we have* $deg(S) \geq 2n - 2$.

Proof. Without loss of generality, consider the left output argument of (1):

$$S_1(x) \oplus S_3(S_1(x) \oplus S_2(y)) = x^{2^n-2} \oplus (x^{2^n-2} \oplus y^{2^n-2})^3$$
$$= x^{2^n-2} \oplus x^{2^n-4} \oplus y^{2^n-4} \oplus x^{2^n-3}y^{2^n-2} \oplus x^{2^n-2}y^{2^n-3}.$$

Since

$$wt(2^n - 3) + wt(2^n - 2) = 2n - 2,$$

so, we have $deg(S) \geq 2n - 2$. □

Remark 3. The proposed structure could be compared with three rounds of a 2-branch Feistel scheme with relevant parameters. Obviously, the resources are the same, but our proposed structure could be parallelized in the computation of $S1$ and S_2, which culminates in a lower latency, as stated in [4].

Example 1. Set $S_1(x) = S_2(x) = x^{-1}$ and $S_3(x) = x^3$ on $\mathbb{F}_{2^4}$, defined by the irreducible polynomial x^4+x+1. It is well-known that $\Delta_{S_1} = \Delta_{S_2} = 4$, $\Delta_{S_3} = 2$, and $\Lambda_{S_1} = \Lambda_{S_2} = \Lambda_{S_3} = 8$. By programming, we see that

$$\Delta_S = 16, \;\; \Lambda_S = 64, \;\; deg(S) = 6.$$

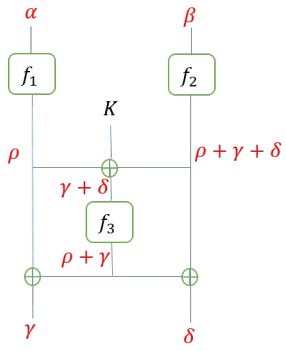

Fig. 3.

3.2 Generalized Lai-Massey Scheme

Here, we propose GLM for the use in symmetric cryptography. As stated before, this structure resembles the structure of the S-boxes used in the FLY block cipher. Note that, we could use this structure either as Figure 4 or Figure 5. One can check that, a relevant form of the following theorems could be proved

for both of them; but, we use the structure in Figure 6, for simplicity. Of course, it is not hard to see that it suffices to prove the theorems for Figure 6, due to the fact that K_1 and K_2 play the role of randomizers between different rounds of GLM and could be omitted, without loss of generality. So, in the rest of the paper, we consider Figure 6.

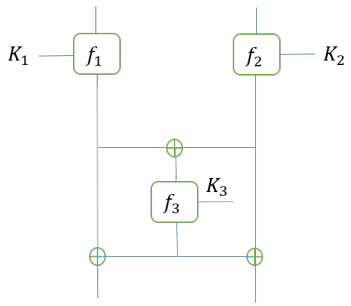

Fig. 4.

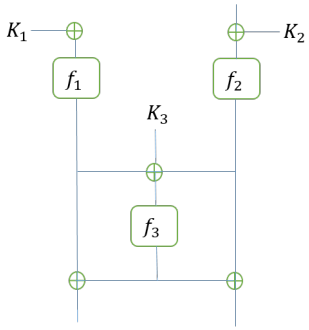

Fig. 5.

Lemma 5. *According to Figure 3, we have:*
a) *The differential pattern* $(\alpha, 0) \to (\gamma, 0)$ *is an impossible differential unless* f_3 *is not a permutation, in which* $DP(F) \leq \mathcal{D}_{f_1}\mathcal{D}_{f_3}$.
b) *Similarly, the differential pattern* $(0, \beta) \to (0, \delta)$ *is either an impossible differential or we have* $DP(F) \leq \mathcal{D}_{f_2}\mathcal{D}_{f_3}$.
c) *For the differential patterns* $(\alpha, 0) \to (\gamma, \delta)$ *and* $(0, \beta) \to (\gamma, \delta)$, *we have* $DP(F) \leq \mathcal{D}_{f_2}\mathcal{D}_{f_3}$ *and* $DP(F) \leq \mathcal{D}_{f_1}\mathcal{D}_{f_3}$, *respectively.*
d) *The differential patterns* $(\alpha, 0) \to (\gamma, \gamma)$ *and* $(0, \beta) \to (\delta, \delta)$ *are impossible differentials.*

e) *For the differential pattern* $(\alpha, \beta) \to (\gamma, \gamma)$*, we have* $DP(F) \leq \mathcal{D}_{f_1}\mathcal{D}_{f_2}$*. Here,* $\mathcal{D}_{f_i} = \frac{\Delta_{f_i}}{2^n}$*,* $1 \leq i \leq 3$*.*

Proof. ***a)*** *According to Figure 3, we have* $\beta = \delta = 0$ *and* $\rho = \gamma$*, which culminates in the differential patterns* $\alpha \to \gamma$ *for* f_1 *and* $\gamma \to 0$ *for* f_3*. Obviously, if* f_3 *is a permutation, we have a contradiction which means that the corresponding pattern is an impossible differential. Now, suppose that* f_3 *is not a permutation: we have*

$$P_x\{F((x,y) \oplus (\alpha, 0), K) \oplus F((x,y), K) = (\gamma, 0)\}$$

$$= P_x\{F((x \oplus \alpha, y), K) \oplus F((x,y), K) = (0, \delta)\}.$$

It follows that:

$$\begin{cases} f_1(x) \oplus f_3(f_1(x) \oplus f_2(y) \oplus K) \oplus f_3(f_1(x \oplus \alpha) \oplus f_2(y) \oplus K) = 0, \\ f_1(x) \oplus f_1(x \oplus \alpha) = \gamma. \end{cases} \tag{2}$$

From the second equation of (2), we have the differential pattern $\alpha \to \gamma$ *for* f_1*. Replacing this equation in the first equation of (2), we get* $f_3(t) \oplus f_3(t \oplus \gamma) = 0$*, where* $t = f_1(x) \oplus f_2(y) \oplus K$*, which culminates in the pattern* $\gamma \to 0$ *for* f_3*. Note that, here, the random key* K *provides the independence of variables. Therefore, we have*

$$DP(F) \leq \mathcal{D}_{f_1}\mathcal{D}_{f_3}.$$

b) *Similar to Case* ***a****.*
c) *Similar to Case* ***a****.*
d) *Consider the pattern* $(\alpha, 0) \to (\gamma, \gamma)$*. According to Figure 3, we have* $\beta = 0$*, which means that* $\rho \oplus \gamma \oplus \delta = 0$*. Since* $\gamma = \delta$*, we have* $\rho = 0$*, which is a contradiction. The proof of impossibility of the differential pattern* $(0, \beta) \to (\delta, \delta)$ *is similar.*
e) *According to Figure 3, we have the patterns* $\alpha \to \rho$ *and* $\beta \to \rho$ *for* f_1 *and* f_2*, respectively. Also, we have* $\gamma = \delta$*. Now, similar to Case* ***a****, we have*

$$DP(F) \leq \mathcal{D}_{f_1}\mathcal{D}_{f_2}.$$

□

Using Lemma 5, we prove the following theorem. This theorem provides a lower bound for MADP of GLM.

Theorem 1. *Suppose that* f_1 *and* f_2 *are invertible maps and* f_3 *is an arbitrary map on* $\mathbb{F}_{2^n}$*. Let* $DP(F)$ *be the MADP of GLM. In this case, we have*

$$DP(F) \leq \min\{\mathcal{D}_{f_1}\mathcal{D}_{f_2}, \mathcal{D}_{f_1}\mathcal{D}_{f_3}, \mathcal{D}_{f_2}\mathcal{D}_{f_3}\}.$$

Proof. For any fixed $K \in \mathbb{F}_{2^n}$*, we have*

$$P_x\{F(x \oplus \Delta x, K) \oplus F(x, K) = \Delta y)\} = \frac{\Delta_F(\Delta x, \Delta y)}{2^{2n}}.$$

According to the definition of $DP(F)$, it suffices to show that for every $K \in \mathbb{F}_{2^n}$,

$$P_x\{F(x \oplus \Delta x, K) \oplus F(x, K) = \Delta y)\} \leq \min\{\mathcal{D}_{f_1}\mathcal{D}_{f_2}, \mathcal{D}_{f_1}\mathcal{D}_{f_3}, \mathcal{D}_{f_2}\mathcal{D}_{f_3}\}.$$

On the other hand, by Figure 3, we have

$$P_x\{F(x \oplus \Delta x, K) \oplus F(x, K) = \Delta y)\} = \frac{\Delta_F(\Delta x, \Delta y)}{2^{2n}}$$

$$= \frac{1}{2^{2n}} \sum_{\rho \in \mathbb{F}_{2^n}} \Delta_{f_1}(\alpha, \rho)\Delta_{f_2}(\beta, \rho + \gamma + \delta)\Delta_{f_3}(\gamma + \delta, \rho + \gamma).$$

Here, $\Delta x = (\alpha, \beta)$ and $\Delta y = (\gamma, \delta)$. Note that, in the above equation, we use the fact that K plays the role of a randomizer and we can use the independence of variables. Since $\sum_{x \in \mathbb{F}_{2^n}} \Delta_{f_2}(\beta, x) = 2^n$. So

$$\sum_{\rho \in \mathbb{F}_{2^n}} \Delta_{f_2}(\beta, \rho + \gamma + \delta) = 2^n.$$

Therefore,

$$\sum_{\rho \in \mathbb{F}_{2^n}} \Delta_{f_1}(\alpha, \rho)\Delta_{f_2}(\beta, \rho+\gamma+\delta)\Delta_{f_3}(\gamma+\delta, \rho+\gamma) \leq \Delta_{f_1}\Delta_{f_3} \sum_{\rho \in \mathbb{F}_{2^n}} D_{f_2}(\beta, \rho+\gamma+\delta)$$

$$\leq 2^n \Delta_{f_1}\Delta_{f_3}.$$

Similarly, it is proved that

$$\sum_{\rho \in \mathbb{F}_{2^n}} \Delta_{f_1}(\alpha, \rho)\Delta_{f_2}(\beta, \rho + \gamma + \delta)\Delta_{f_3}(\gamma + \delta, \rho + \gamma) \leq 2^n \Delta_{f_1}\Delta_{f_2},$$

and

$$\sum_{\rho \in \mathbb{F}_{2^n}} \Delta_{f_1}(\alpha, \rho)\Delta_{f_2}(\beta, \rho + \gamma + \delta)\Delta_{f_3}(\gamma + \delta, \rho + \gamma) \leq 2^n \Delta_{f_2}\Delta_{f_3}.$$

Now, by Lemma 5 (refrain from the impossible differentials) we have

$$DP(F) \leq \min\{\mathcal{D}_{f_1}\mathcal{D}_{f_2}, \mathcal{D}_{f_1}\mathcal{D}_{f_3}, \mathcal{D}_{f_2}\mathcal{D}_{f_3}\}. \ \square$$

Corollary 1. *In Theorem 1, if $f_1 = f_2 = f_3 = f$, then $DP(F) \leq \mathcal{D}_f^2$.*

Corollary 2. *The differential patterns $(\alpha, 0) \to (\gamma, \gamma)$ and $(0, \beta) \to (\delta, \delta)$ are impossible differentials for GLM. In the case that f_3 is a permutation, the patterns $(\alpha, 0) \to (\gamma, 0)$ and $(0, \beta) \to (0, \delta)$ are also impossible differentials.*

Corollary 3. *According to Corollary 2, it is simply proved that two rounds of GLM do not have any (structural) impossible differentials.*

The proof of next lemma is similar to Lemma 5.

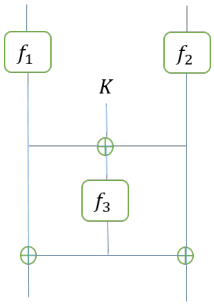

Fig. 6.

Lemma 6. *We have:*
a) *The linear pattern* $(\alpha, 0) \to (\gamma, 0)$ *is a zero-correlation unless* f_3 *is not a permutation, in which*

$$LP(F) \leq \mathcal{C}_{f_1}\mathcal{C}_{f_3}.$$

b) *Similarly, the linear pattern* $(0, \beta) \to (0, \delta)$ *is a zero-correlation unless* f_3 *is not a permutation, in which*

$$LP(F) \leq \mathcal{C}_{f_2}\mathcal{C}_{f_3}.$$

c) *For the linear patterns* $(\alpha, 0) \to (\gamma, \delta)$ *and* $(0, \beta) \to (\gamma, \delta)$*, we have* $LP(F) \leq \mathcal{C}_{f_1}\mathcal{C}_{f_3}$ *and* $LP(F) \leq \mathcal{C}_{f_2}\mathcal{C}_{f_3}$*, respectively.*
d) *The linear patterns* $(\alpha, 0) \to (\gamma, \gamma)$ *and* $(0, \beta) \to (\delta, \delta)$ *are zero-correlations.*
e) *For the linear pattern* $(\alpha, \beta) \to (\gamma, \gamma)$*, we have* $LP(F) \leq \mathcal{C}_{f_1}\mathcal{C}_{f_2}$.

The proof of the next theorem is done in the same manner as Theorem 1.

Theorem 2. *Suppose that* f_1 *and* f_2 *are permutations and* f_3 *is an arbitrary map on* $\mathbb{F}_{2^n}$*. Let* $LH(F)$ *is the MALH of GLM. In this case, we have*

$$LH(F) \leq \min\{\mathcal{C}_{f_1}\mathcal{C}_{f_2}, \mathcal{C}_{f_1}\mathcal{C}_{f_3}, \mathcal{C}_{f_2}\mathcal{C}_{f_3}\}.$$

Corollary 4. *The linear patterns* $(\alpha, 0) \to (\gamma, \gamma)$ *and* $(0, \beta) \to (\delta, \delta)$ *are zero-correlations for GLM. In the case that* f_3 *is a permutation, the patterns* $(\alpha, 0) \to (\gamma, 0)$ *and* $(0, \beta) \to (0, \delta)$ *are also zero-correlations.*

Corollary 5. *Lemma 6 shows that, two rounds of GLM do not have (structural) zero-correlations.*

Remark 4. As we stated in Remark 3 and according to Theorem 1 and Theorem 2, GLM could be compared with a three-round (two-branch classic) Feistel scheme: On one hand, the provable security of both of them has similar results and both of them need the same resources. On the other hand, the first layer in GLM could be parallely implemented; which is an important advantage in hardware and/or software implementations.

3.3 Pseudo-Randomness of GLM

In this subsection, we prove the pseudo-randomness of GLM. Firstly, we give some notations and facts which are used to prove the pseudo-randomness of GLM. The following theorem is proved in [10].

Theorem 3. *Let N and q be natural and α and β be real numbers, with $\alpha, \beta > 0$. Let E be a subset of $\mathbb{F}_2^{Nq}$ such that $|E| \geq (1-\beta)2^{Nq}$. If*
(1) For all sequences a_i, $1 \leq i \leq q$, of pairwise distinct elements of $\mathbb{F}_2^N$ and for all sequences b_i, $1 \leq i \leq q$, of E, we have

$$H \geq \frac{|K|}{2^{Nq}}(1-\alpha),$$

Then,
(2) For every CPA with q chosen plaintexts, we have: $Adv^{CPA} \leq \alpha + \beta$.

Here, CPA stands for chosen plaintext attack and Adv^{CPA} is the advantage of a random distinguisher with q, CPA queries (cf Definition 1.3 [10]). In the next theorem, we prove the pseudo-randomness of GLM.

Theorem 4. *Let q be a natural number and (L_i, R_i) and (S_i, T_i), $1 \leq i \leq q$, be distinct inputs and outputs of GLM, respectively. Then, there are H number of 3-tuples of (f_1, f_2, f_3) such that f_1 and f_2 are random permutations and f_3 is a random mapping on $\mathbb{F}_2^n$ and*

$$\begin{aligned} f_1(L_i) \oplus f_3(f_1(L_i) \oplus f_2(R_i)) &= S_i, \\ f_2(R_i) \oplus f_3(f_1(L_i) \oplus f_2(R_i)) &= T_i. \end{aligned} \tag{3}$$

where, $1 \leq i \leq q$, and

$$H \geq \frac{|F_n||P_n|^2}{2^{2nq}}(1 - \frac{q(q-1)}{1^{n+1}}).$$

Proof. Fix $1 \leq i < j \leq q$. We distinguish two cases:
a) $L_i = L_j$: which means that $R_i \neq R_j$. In this case, there are at most $2^n!(2^n-1)!$ permutations f_1 and f_2 such that

$$f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j).$$

b) $L_i \neq L_j$: in this case, either $R_i = R_j$ whose proof is similar to Case a, or $R_i \neq R_j$, in which we have at most $(2^n-1)!^2$ permutations f_1 and f_2 such that

$$f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j).$$

Therefore, in both cases there are at most $2^n!(2^n-1)!^{\frac{q(q-1)}{2}}$ permutations f_1 and f_2 such that for some (i,j), $1 \leq i < j \leq q$, we have

$$f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j).$$

So, there are at least $2^n!^2 - 2^n!(2^n-1)!^{\frac{q(q-1)}{2}}$ permutations f_1 and f_2 such that the values of $f_1(L_i) \oplus f_2(R_i)$ are not equal to $f_1(L_j) \oplus f_2(R_j)$, for some (i,j),

$1 \leq i < j \leq q$.
For fixed $1 \leq i \leq q$ *and every* f_1 *and* f_2 *satisfying* (3)*, there are at least* $\frac{2^{n2^n}}{2^{2n}}$ *mappings* f_3 *for which* (3) *holds. Thus, we have at least* $\frac{2^{n2^n}}{2^{2nq}}$ *mappings* f_3 *satisfying* (3)*, for every* $1 \leq i \leq q$*. Therefore,*

$$H \geq (2^n!^2 - 2^n!(2^n-1)!\frac{q(q-1)}{2})\frac{2^{n2^n}}{2^{2nq}}$$

$$= \frac{2^n!^2 2^{n2^n}}{2^{2nq}}(1 - \frac{q(q-1)}{2^{n+1}})$$

$$= \frac{|F_n||P_n|^2}{2^{2nq}}(1 - \frac{q(q-1)}{2^{n+1}}).\square$$

Theorem 4 proves the pseudo-randomness of GLM against chosen plaintext attacks (security against CPA). By Theorem 4, the proof of next corollary is straightforward.

Corollary 6. *For every* CPA *with* q *queries, we have*

$$Adv^{CPA} \leq \frac{q^2}{2^n}.$$

4 Conclusion

In this paper, based upon the S-box proposed in the Fly cipher, we study the cryptographic properties of S-boxes constructed via this structure. Then, we propose a new cipher structure (GLM) and investigate MADP and MALH of the proposed structure. We present impossible differentials and zero-correlations for one round of this structure and prove that there are no structural impossible differentials and zero-correlations for two rounds of GLM. Finally, we prove the pseudo-randomness of GLM.
Regarding the upper bounds for MADP and MALH, GLM is comparable to three rounds of a classic Feistel scheme. An advantage of our proposed structure over the Feistel scheme is that the first layer of GLM could be implemented in parallel, which is faster in software and hardware implementations.

References

1. R. Beaulieu, D. Shores, J. Smith, S. Treatman Clark, B. Weeks and L. Wingers. *The SIMON and SPECK families of lightweight block ciphers.* IACR cryptology ePrint Archive, 2013: 404,2013.
2. *Data Encryption Standard (DES).* Federal Information Processing Standard (FIPS) Publication 46, 1977.
3. P. Junod and S. Vaudenay. *FOX: A new family of block ciphers.* SAC 2004, pp 114-129, 2004.
4. P. Karpman. *Exercice de style.* 2016: hal-01263735.

5. *ETSI. TS 135 202 V7.0.0: Universal mobile telecommunications system (UMTS); specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification (3GPP TS 35.202 version 7.0.0 Release 7).*
6. X. Lai and J. L. Massey. *A proposal for a new block encryption standard.* EUROCRYPT 90, pp 389-404, 1991.
7. C. H. Lim and H. S. Hwang. *CRYPTON: A new 128-bit block cipher - specification and analysis.* Submitted as candidate for AES, 1997.
8. M. Matsui. *New block encryption algorithm MISTY.* FSE 97, pp 54-68, 1997.
9. S. Miyaguchi. *The FEAL-8 cryptosystem and a call for attack.* CRYPTO 89, volume 435 of Lecture Notes in Computer Science, Springer, pages 624627, 1990.
10. V. Nachef, J. Patarin and E. Volte. *Feistel Ciphers, Security Proofs and Cryptanalysis.* Springer, 2017.
11. J. Nakahara, V. Rijmen, B. Preneel and J. Vandewalle. *The MESH block ciphers.* WISA 2003, pp 458-473, 2003.
12. *SKIPJACK and KEA algorithm specifications.* National Security Agency (NSA), 1998.
13. J. Stern and S. Vaudenay. *CS-cipher.* FSE 98, pp 189-205, 1998.
14. *ETSI SAGE: Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 128-EIA3 Document 2: ZUC Specification.* Version 1.5, 4th January 2011.