Practical Security Evaluation against Differential and Linear Cryptanalyses for the Lai-Massey Scheme with an SPS *F*-function

Lishi Fu[1], Chenhui Jin[1]
[1] Information Science and Technology Institute
Zhengzhou, 450001, China
[email: fulishi123@sohu.com, jinchenhui@126.com]

Received October 29, 2012; revised November 15, 2013; accepted July 21, 2014; published October 31, 2014

Abstract

At SAC 2004, Junod and Vaudenay designed the FOX family based on the Lai-Massey scheme. They noted that it was impossible to find any useful differential characteristic or linear trail after 8 rounds of FOX64 or FOX128. In this paper, we provide the lower bound of differentially active *S*-boxes in consecutive rounds of the Lai-Massey scheme that has SPS as its *F*-function, and we propose the necessary conditions for the reachability of the lower bound. We demonstrate that similar results can be obtained with respect to the lower bound of linearly active *S*-boxes by proving the duality in the Lai-Massey scheme. Finally, we apply these results to FOX64 and FOX128 and prove that it is impossible to find any useful differential characteristics or linear trail after 6 rounds of FOX64. We provide a more precise security bound for FOX128.

Keywords: Lai-Massey, differentially active *S-boxes*, linearly active *S-boxes*, duality, SPS network

This research was supported by National Natural Science Foundation of China (Grant No. 61272488). We express our thanks to Dr. Ting Cui and Dr Rui Guo who helped us to improve the quality of this manuscript. We are also grateful to the anonymous referees for their valuable comments.

http://dx.doi.org/10.3837/tiis.2014.10.020

1. Introduction

One of the most important parts of the block cipher is the high level, as it will directly affect the implementation performance and choice of round numbers. Among all of the high levels, the Lai-Massey scheme is well known for its simplicity and security. This scheme was first proposed by Lai and Massey in 1991, and it was used in the design of IDEA [1]. Since its inception, the Lai-Massey scheme has attracted considerable attention worldwide. In Asiacrypt '99, Vaudenay added a simple function σ, which has the orthomorphic or α-almost orthomorphic property, to one branch of each round (**Fig. 1**) [2]. Junod and Vaudenay adopted this modified scheme and designed the FOX family (**Fig. 2**) [3]. In 2005, FOX was announced by MediaCrypt under the name of IDEA NXT.

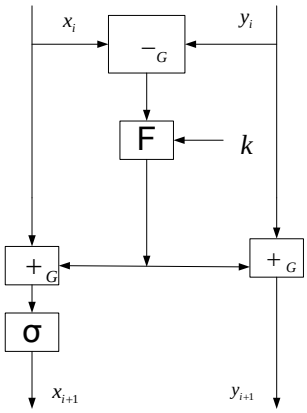

Fig. 1. The (extended) Lai-Massey Scheme

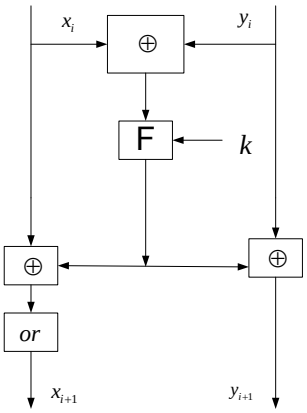

Fig. 2. The Outline of FOX

Various attack methods have been applied to FOX [4-8]. The best-known attacks against block ciphers are the differential cryptanalysis [9] and the linear cryptanalysis [10]. Designers should evaluate the security of any new proposed ciphers against these two cryptanalyses because they are the most powerful approaches available for attacking many symmetric block ciphers. In [11], Kanda et al. noted that the security of a cipher could be evaluated against these two cryptanalyses by upper-bounding the maximum differential characteristic and linear trail probabilities. For most block ciphers, the only nonlinear part is the *S*-boxes, and thus, the upper bounds of the maximum differential characteristic and linear trail probabilities are due to the lower bounds of the differentially and linearly active *S*-boxes in some consecutive rounds.

For SPS structures, Rijmen et al. introduced the branch number [12], which is the lower bound of differentially (or linearly) active *S*-boxes. Because the basic framework of the round function in FOX is an SPS structure, Junod and Vaudenay proposed the lower bound of differential (or linear) *S*-boxes in FOX via providing the lower bound of differentially (or linearly) active round functions [3]. However, according to our observations, the lower bound provided by [3] cannot be obtained when the round number is greater than 3, indicating that the lower bound provided by [3] could be improved.

This paper focuses on finding a tighter bound of active *S*-boxes in some consecutive rounds of the Lai-Massey scheme with an SPS *F*–function, and then, this result is used to improve the lower bound provided in [3]. Thus, we improve the results stated in [3] by Junod and

Vaudenay, who mentioned that at least 8 rounds of FOX64 can provide resistance against traditional differential and linear cryptanalyses. However, the result obtained here indicates that 6 rounds are sufficient for FOX64.

This paper is organized as follows. Section 2 introduces some notations and definitions, Section 3 studies the lower bound of differentially active *S*-boxes in the Lai-Massey scheme with an SPS *F*-function, and Section 4 provides the duality in the Lai-Massey scheme and obtains the lower bound of its linearly active *S*-boxes. In addition, we apply these results to FOX64 and FOX128 in Section 4. Finally, the conclusions of this study are provided in Section 5.

2. Preliminaries

This section presents some notations and definitions.

Throughout this paper, we will use the following symbols:

Å XOR operation;

$+$ addition over the real number space;

$+_G$ the addition operation over group G;

$-_G$ the inverse operation of $+_G$;

$Hw(x)$ the number of nonzero components in vector x;

P^T the transpose of matrix P;

$a \square b$ the parity of the bitwise XOR of vectors α and b;

P^{-1} the inverse of matrix P.

Definition 1[2] Let $(G,+_G)$ be a group, let $F_1,F_2,\cdots,F_r$ be r functions on G, and let σ be a permutation on G. We define an r-round Lai-Massey scheme as a permutation $\Lambda^\sigma(F_1,F_2,\cdots,F_r)$ on G^2 by

$$\Lambda^\sigma(F_1,F_2,\cdots,F_r)(x,y)=\Lambda^\sigma(F_2,\cdots,F_r)(\sigma(x+_G F(x-_G y)),y+_G F(x-_G y))$$

and

$$\Lambda^\sigma(F_r)(x,y)=(x+_G F(x-_G y),y+_G F(x-_G y))$$

in which the last σ is omitted.

In the sequel, we assume the group is $(\{0,1\}^n,\oplus)$. For convenience, we denote $F_1,F_2,\cdots,F_r$ as F such that the round function can be written as

$$Q(x_i,y_i)=(\sigma(x_i\oplus F(x_i\oplus y_i)),y_i\oplus F(x_i\oplus y_i)).$$

Definition 2[13] Let $f:\{0,1\}^n\to\{0,1\}^m$, and let $\alpha\in\{0,1\}^n,\beta\in\{0,1\}^m$. Then,

$$p_f(\alpha\to\beta)=\frac{1}{2^n}\#\{x\in\{0,1\}^n: f(x\oplus\alpha)\oplus f(x)=\beta\}$$

and

$$W_{(f)}(\alpha\to\beta)=\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{\beta\square f(x)\oplus\alpha\square x}$$

are called the probabilities of the differential $\alpha\to\beta$ for f and the linear approximation $\alpha\to\beta$ for f respectively.

Definition 3[2] Let $f:\{0,1\}^n\to\{0,1\}^n$ be a mapping. Then, f is called an orthomorphism if both $f(x)$ and $g(x)=f(x)\oplus x$ are bijective.

Definition 4[14] An *S*-box (resp. *F*) is called differentially active if its input difference is

nonzero, and an *S*-box (resp. *F*) is called linearly active if its output mask value is nonzero.

Note: When an *S*-box is bijective, an *S*-box with a non-zero output difference is also a differentially active *S*-box. Similarly, when an *F*-box is bijective, it is linearly active if it has a non-zero input mask value.

Definition 5 Let $\sigma(x) = Mx \oplus C$ be an orthomorphism. Then, the Lai-Massey scheme with $\sigma_D(x) = (M^{-1})^T x \oplus C$ as its σ is called the dual scheme for the Lai-Massey scheme with $\sigma(x) = Mx \oplus C$ as its σ.

Definition 6[12] For the diffusion layer P, the relationship between the input difference and output difference is represented by matrix *P*, i.e., $\Delta y = P\Delta x$. Furthermore, the relationship between the output and input mask values is represented by P^T; thus, $\Gamma x = P^T \Gamma y$. In addition, the values $B_d(P) = \min_{\Delta x \neq 0}\{Hw(\Delta x) + Hw(P\Delta x)\}$ and $B_l(P) = \min_{\Gamma x \neq 0}\{Hw(\Gamma y) + Hw(P^T \Gamma y)\}$ are called the differential branch number and linear branch number, respectively.

3. Lower Bound of Differentially Active *S-boxes* in the Lai-Massey Scheme with an SPS *F*-function

First, we will study the relationship between the differential of the round function and the differentials of the *F*-function and σ permutation.

Theorem 1 The probability of the differential $(\alpha, \beta) \to (A, B)$ of the round function *Q* is nonzero iff the differentials for *F* and σ are $\alpha \oplus \beta \to \beta \oplus B$ and $\alpha \oplus \beta \oplus B \to A$, respectively, and the probabilities of these two differentials are both nonzero. Moreover,

$$p_Q((\alpha, \beta) \to (A, B)) = p_F(\alpha \oplus \beta \to \beta \oplus B)\, p_\sigma(\alpha \oplus \beta \oplus B \to A).$$

In particular, if $\sigma(x) = \delta(x) \oplus \sigma(0)$ is affine, then the output difference of *F* is $\beta \oplus B = \alpha \oplus \delta^{-1}(A)$.

Proof See Appendix A.

For the SPS structure, according to [13], the lower bound of the active *S*-boxes is listed in lemma 1.

Lemma 1[13] In the SPS structure, let *S* be bijective and let the differential branch and linear branch of *P* be B_d and B_l, respectively. The number of differentially active *S*-boxes is at least B_d if the input difference is nonzero, and the number of linearly active *S*-boxes is at least B_l if the output mask is nonzero.

For the Lai-Massey scheme, the lower bound of the active *F*-functions is given in lemma 2 below.

Lemma 2 Let σ be an orthomorphism. Then, a consecutive 2-round differential characteristic for the Lai-Massey scheme with nonzero probability contains at least one active *F* -function.

Proof Let $(\alpha, \beta) \to (A, B) \to (u, v)$ be a consecutive 2-round differential characteristic for the Lai-Massey scheme. Lemma 1 indicates that the differentials for *F* and σ in the first round are $\alpha \oplus \beta \to \beta \oplus B$ and $\alpha \oplus \beta \oplus B \to A$, respectively, and the differentials for *F* and σ in the second round are $A \oplus B \to B \oplus v$ and $A \oplus B \oplus v \to u$, respectively.

If the *F*-function is not active in the first round, then $\alpha = \beta$ and $\alpha = \beta = B$; if *F* is not active in the second round, then $A = B$ and $A = B = v$. Therefore, the differential for *F* in the first round's function is $A \to A$. Because $(A, B) \neq (0, 0)$ and $A = B$, $A \neq 0$, $p_\sigma(A \to A) = 0$ if σ is an orthomorphism according to lemma 1. Moreover, theorem 1 indicates that

$p_Q((\alpha,\beta)\to(A,B))=0$, which contradicts the fact that the probability is nonzero. Therefore, a consecutive two-round differential characteristic with nonzero probability contains at least one active *F* -function.

Q.E.D

For the Lai-Massey scheme with an SPS *F*-function, the corollary below follows from lemmas 1 and 2 because there are at least B_d differentially (B_l linearly) active *S*-boxes in one active *F*-function.

Corollary For the Lai-Massey scheme with an SPS *F* -function, let the differential and linear branches of *P* be B_d and B_l, respectively. Then, there are at least nB_d differential (nB_l linear) active *S*-boxes in 2*n* consecutive rounds.

Remarks: Let B_d and B_l be odd. Then, for the nontrivial differential (linear approximation) $\alpha\to\alpha$ of an SPS structure, there are at least B_d+1 (B_l+1) *S*-boxes that will be active after a *P*-permutation. Based on this fact, we make some improvement on the corollary of lemma 2. First, we consider the number of active *S*-boxes in 3 consecutive rounds, where $B_d\geq 3$ and $B_l\geq 3$.

Theorem 2 For the Lai-Massey scheme with an SPS *F*-function, let B_d be odd and let $\sigma(x)=\delta(x)\oplus\sigma(0)$ be an affine orthomorphsim. Then, there are at least B_d+1 active *S*-boxes in a 3-round differential characteristic iff the structure is

$$(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\alpha),\delta(\alpha))\to(\delta^2(\alpha),\delta(\alpha))$$

and the corresponding differentials for *F* are $0\to 0$, $\delta(\alpha)\oplus\alpha\to\delta(\alpha)\oplus\alpha$, and $0\to 0$, respectively. Here, $Hw(\delta(\alpha)\oplus\alpha)=(B_d+1)/2$.

Proof If there are at least two active *F*-functions in the 3-round differential characteristic, this chain contains at least $2B_d$ active *S*-boxes according to lemma 2. If there is only one active *F*-function in the 3-round differential characteristic, the structure of this differential characteristic is $(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\alpha),\delta(\alpha))\to(\delta^2(\alpha),\delta(\alpha))$ and the corresponding differentials for *F* are $0\to 0$, $\delta(\alpha)\oplus\alpha\to\delta(\alpha)\oplus\alpha$, and $0\to 0$, respectively, where $\alpha\neq 0$, according to theorem 1. Because B_d is odd, the differential $\delta(\alpha)\oplus\alpha\to\delta(\alpha)\oplus\alpha$ for the SPS structure contains at least B_d+1 active *S*-boxes, where $Hw(\delta(\alpha)\oplus\alpha)=(B_d+1)/2$.

Q.E.D.

In the sequel, $AS^{(a\to b)}$ denotes the number of active *S*-boxes in the differential characteristic from the *a*th to *b*th round, and $AS^{(a)}$ denotes the number of active *S*-boxes in the *a*th round.

Theorem 3 For the Lai-Massey scheme with an SPS *F*-function, let $B_d\geq 3$ be odd and let $\sigma(x)=\delta(x)\oplus\sigma(0)$ be an affine orthomorphsim.

(1) There are at least $Low_D^{(r)}$ ($r\geq 3$) active *S*-boxes in an *r*-round differential characteristic, where

$$Low_D^{(r)}=\begin{cases}(r-1)(B_d+1)/2, & \textit{if } r \textit{ is odd};\\ (r/2-2)(B_d+1)+2B_d, & \textit{if } r \textit{ is even}.\end{cases}$$

(2) If the number of active *S*-boxes is $Low_D^{(r)}$ in the *r*-round differential characteristic, then the *F*-functions in the first and last rounds are non-active.

Proof According to theorem 2, this theorem is true for $r=3$. Next, we use induction to prove this theorem.

Suppose that (1) and (2) are true for $r\leq 2m+1$. For $r=2m+2$, the number of active *S*-boxes

in the first round is at least B_d if the *F*-function in the first round is active. By inductive supposition we have that $AS^{(2\to 2m+2)} \geq m(B_d+1)$. Hence,

$$\begin{aligned} AS^{(1\to 2m+2)} &= AS^{(1)} + AS^{(2\to 2m+2)} \\ &\geq (m-1)(B_d+1) + 2B_d + 1 \\ &> (m-1)(B_d+1) + 2B_d. \end{aligned}$$

A similar proof can be provided for the case in which the *F*-function in the last round is active, i.e., that $AS^{(1\to 2m+2)} > (m-1)(B_d+1)+2B_d$. Therefore, (2) is true for $r = 2m+2$.

We now consider the case that the *F*-function is active in neither the first nor last round. Two cases are stated below based on whether the *F*-function in the $m+2$ th round is active or not.

Case 1: Suppose that *F* is not active in the $m+2$ th round; then, we have

$$AS^{(m+2\to 2m+2)} = AS^{(m+2)} + AS^{(m+3\to 2m+2)} = AS^{(m+3\to 2m+2)}.$$

Therefore, $AS^{(1\to 2m+2)} = AS^{(1\to m+2)} + AS^{(m+3\to 2m+2)} = AS^{(1\to m+2)} + AS^{(m+2\to 2m+2)}$.

If *m* is odd, $AS^{(m+2\to 2m+2)} = [(m+1)/2-2](B_d+1)+2B_d$ and $AS^{(1\to m+2)} \geq (m+1)(B_d+1)/2$ by inductive supposition; therefore,

$$\begin{aligned} AS^{(1\to 2m+2)} &\geq (m+1)(B_d+1)/2 + [(m+1)/2-2](B_d+1) + 2B_d \\ &= (m-1)(B_d+1) + 2B_d. \end{aligned}$$

If *m* is even, $AS^{(1\to m+2)} \geq (m/2-1)(B_d+1)+2B_d$ and $AS^{(m+2\to 2m+2)} \geq (m/2)(B_d+1)$ by the supposition; therefore,

$$\begin{aligned} AS^{(1\to 2m+2)} &\geq [(m/2-1)(B_d+1)+2B_d] + (m/2)(B_d+1) \\ &= (m-1)(B_d+1) + 2B_d. \end{aligned}$$

This result indicates that (1) is true for $r = 2m+2$ when the *F*-function in the $m+2$ th round is non-active.

Case 2: Suppose that the *F*-function in the $m+2$ th round is active. Then, we can demonstrate that $AS^{(2m+2)} = AS^{(1\to m+1)} + AS^{(m+2)} + AS^{(m+3\to 2m+2)}$.

If *m* is odd, then by the inductive supposition,

$$AS^{(1\to m+1)} \geq [(m+1)/2-2](B_d+1)+2B_d,\ AS^{(m+3\to 2m+2)} \geq (m-1)(B_d+1)/2.$$

If $AS^{(1\to m+1)} = [(m+1)/2-2](B_d+1)+2B_d$ and $AS^{(m+3\to 2m+2)} = (m-1)(B_d+1)/2$, then $AS^{(m+1)} = AS^{(m+3)} = 0$ by (2) in the supposition. Moreover, considering the implications of theorem 2, we have $AS^{(m+2)} = AS^{(m+1\to m+3)} \geq B_d + 1$; thus,

$$\begin{aligned} AS^{(1\to 2m+2)} &= AS^{(1\to m+1)} + AS^{(m+2)} + AS^{(m+3\to 2m+2)} \\ &= AS^{(1\to m+1)} + AS^{(m+1\to m+3)} + AS^{(m+3\to 2m+2)} \\ &\geq [(m+1)/2-2](B_d+1) + 2B_d + B_d + 1 + (m-1)(B_d+1)/2 \\ &= (m-1)(B_d+1) + 2B_d. \end{aligned}$$

If $AS^{(1\to m+1)}$ and $AS^{(m+3\to 2m+1)}$ cannot reach the minimum number simultaneously, then

$$\begin{aligned} AS^{(1\to m+1)} + AS^{(m+3\to 2m+2)} &\geq [(m+1)/2-2](B_d+1) + 2B_d + (m-1)(B_d+1)/2 + 1 \\ &= (m-1)(B_d+1) + B_d. \end{aligned}$$

Because the *F*-function in the $m+2$-th round is active, we have $AS^{(m+2)} \geq B_d$. Hence,

$$\begin{aligned} AS^{(1\to 2m+2)} &= AS^{(1\to m+1)} + AS^{(m+3\to 2m+2)} + AS^{(m+2)} \\ &\geq (m-1)(B_d+1) + B_d + B_d = (m-1)(B_d+1) + 2B_d. \end{aligned}$$

Thus, (1) is true for $r = 2m+2$ when *m* is odd.

If *m* is even, then by the inductive supposition,

$$AS^{(1\to m+1)} \ge (m/2)(B_d+1),\ AS^{(m+3\to 2m+2)} \ge (m/2-2)(B_d+1)+2B_d.$$

If $AS^{(1\to m+1)} = (m/2)(B_d+1)$ and $AS^{(m+3\to 2m+2)} = (m/2-2)(B_d+1)+2B_d$, then $AS^{(m+1)} = AS^{(m+3)} = 0$ by (2) in the supposition. Moreover, $AS^{(m+2)} = AS^{(m+1\to m+3)} \ge B_d+1$ according to theorem 2. Hence,

$$\begin{aligned} AS^{(1\to 2m+2)} &= AS^{(1\to m+1)} + AS^{(m+2)} + AS^{(m+3\to 2m+2)} \\ &= AS^{(1\to m+1)} + AS^{(m+1\to m+3)} + AS^{(m+3\to 2m+2)} \\ &\ge (m/2)(B_d+1) + B_d + 1 + (m/2-2)(B_d+1)/2 + 2B_d \\ &= (m-1)(B_d+1) + 2B_d \end{aligned}$$

If $AS^{(1\to m+1)}$ and $AS^{(m+3\to 2m+1)}$ cannot reach the minimum number simultaneously, then

$$\begin{aligned} AS^{(1\to m+1)} + AS^{(m+3\to 2m+2)} &\ge (m/2)(B_d+1) + (m/2-2)(B_d+1)/2 + 2B_d + 1 \\ &= (m-1)(B_d+1) + B_d. \end{aligned}$$

Because the *F*-function in the $m+2$ th round is active, we have $AS^{(m+2)} \ge B_d$ Hence,

$$\begin{aligned} AS^{(1\to 2m+2)} &= AS^{(1\to m+1)} + AS^{(m+3\to 2m+2)} + AS^{(m+2)} \\ &\ge (m-1)(B_d+1) + B_d + B_d \\ &= (m-1)(B_d+1) + 2B_d. \end{aligned}$$

Thus, (1) is true for $r = 2m+2$ when m is even. Therefore, (1) is true for $r = 2m+2$ if the *F*-function in the $m+2$ th round is active.

Cases 1 and 2 demonstrate that (1) is true for $r = 2m+2$ if it is true for $r \le 2m+1$.

Next, suppose that (1) and (2) are true for $r \le 2m$. For $r = 2m+1$, $AS^{(1)} \ge B_d$ if the *F*-function in the first round is active, and $AS^{(2\to 2m+1)} \ge (m-2)(B_d+1)+2B_d$ according to (2) in the inductive supposition. As a result,

$$AS^{(1\to 2m+1)} \ge B_d + (m-2)(B_d+1) + 2B_d = m(B_d+1) + B_d - 2 > m(B_d+1).$$

Similarly, $AS^{(1\to 2m+1)} > m(B_d+1)$ if the *F*-function in the last round is active. Therefore, (2) is true for $r = 2m+1$.

Next, we consider the case in which neither the *F*-function in the first round nor the *F*-function in the last round is active. Two cases are listed below according to whether the *F*-function in the $m+2$ th round is active or not.

Case 1: Suppose that *F* in the $m+2$ th round is not active. Then, we have

$$AS^{(m+2\to 2m+1)} = AS^{(m+2)} + AS^{(m+3\to 2m+1)} = AS^{(m+3\to 2m+1)};$$

therefore, $AS^{(1\to 2m+1)} = AS^{(1\to m+2)} + AS^{(m+2\to 2m+1)}$.

If *m* is odd, then $AS^{(m+2\to 2m+1)} \ge (m-1)(B_d+1)/2$ and $AS^{(1\to m+2)} \ge (m+1)(B_d+1)/2$ by inductive supposition. Therefore,

$$AS^{(1\to 2m+1)} \ge (m+1)(B_d+1)/2 + (m-1)(B_d+1)/2 = m(B_d+1).$$

If *m* is even, then, by the supposition, we have

$$AS^{(1\to m+2)} \ge (m/2-1)(B_d+1)+2B_d,\ AS^{(m+2\to 2m+1)} \ge (m/2-2)(B_d+1)+2B_d.$$

Thus,

$$\begin{aligned} AS^{(1\to 2m+1)} &\ge [(m/2-1)(B_d+1)+2B_d] + (m/2-2)(B_d+1)+2B_d \\ &= (m-3)(B_d+1)+4B_d. \end{aligned}$$

Moreover, as $(m-2)(B_d+1)+4B_d \ge m(B_d+1)$ is equivalent to $B_d \ge 3$, then $AS^{(1\to 2m+1)} \ge (m-3)(B_d+1)+4B_d \ge m(B_d+1)$, which indicates that (1) is true for $r = 2m+1$.

Case 2: If the *F*-function in the $m+2$ th round is active, then $AS^{(2m+1)} = AS^{(1\to m+1)} + AS^{(m+2)} + AS^{(m+3\to 2m+1)}$.

If m is odd, by inductive supposition,

$$AS^{(1\to m+1)} \geq [(m+1)/2-2](B_d+1)+2B_d,\ AS^{(m+3\to 2m+1)} \geq [(m-1)/2-2](B_d+1)+2B_d.$$

If $AS^{(1\to m+1)}$ and $AS^{(m+3\to 2m+1)}$ make the equality true simultaneously, then $AS^{(m+1)} = AS^{(m+3)} = 0$ by (2) in the inductive supposition. Moreover, $AS^{(m+2)} = AS^{(m+1\to m+3)} \geq B_d+1$ according to theorem 2. Hence,

$$\begin{aligned} AS^{(1\to 2m+1)} &= AS^{(1\to m+1)} + AS^{(m+2)} + AS^{(m+3\to 2m+1)} \\ &= AS^{(1\to m+1)} + AS^{(m+1\to m+3)} + AS^{(m+3\to 2m+1)} \\ &\geq [(m+1)/2-2](B_d+1)+2B_d+B_d+1+[(m-1)/2-2](B_d+1)+2B_d \\ &= m(B_d+1)+B_d-3 \geq m(B_d+1). \end{aligned}$$

If $AS^{(1\to m+1)}$ and $AS^{(m+3\to 2m+1)}$ cannot make the equality true simultaneously, then

$$\begin{aligned} &AS^{(1\to m+1)} + AS^{(m+3\to 2m+1)} \\ &\geq [(m+1)/2-2](B_d+1)+2B_d+[(m-1)/2-2](B_d+1)+2B_d+1 \\ &= (m-4)(B_d+1)+4B_d+1. \end{aligned}$$

$AS^{(m+2)} \geq B_d$ because the F-function in $m+2$ th round is active; therefore,

$$\begin{aligned} AS^{(1\to 2m+1)} &= AS^{(1\to m+1)} + AS^{(m+3\to 2m+1)} + AS^{(m+2)} \\ &\geq (m-4)(B_d+1)+4B_d+1+B_d \\ &= m(B_d+1)+B_d-3 \geq m(B_d+1). \end{aligned}$$

This result indicates that when m is odd, (1) is true for $r = 2m+1$.

If m is even, by inductive supposition, we have

$$AS^{(1\to m+1)} \geq (m/2)(B_d+1),\ AS^{(m+3\to 2m+1)} \geq (m-2)(B_d+1)/2.$$

If $AS^{(1\to m+1)}$ and $AS^{(m+3\to 2m+1)}$ make the equality true simultaneously, we obtain $AS^{(m+1)} = AS^{(m+3)} = 0$ by (2) in the supposition, and thus, $AS^{(m+2)} = AS^{(m+1\to m+3)} \geq B_d+1$ according to theorem 2. Hence,

$$\begin{aligned} AS^{(1\to 2m+1)} &= AS^{(1\to m+1)} + AS^{(m+2)} + AS^{(m+3\to 2m+1)} \\ &= AS^{(1\to m+1)} + AS^{(m+1\to m+3)} + AS^{(m+3\to 2m+1)} \\ &\geq (m/2)(B_d+1)+B_d+1+(m-2)(B_d+1)/2 = m(B_d+1). \end{aligned}$$

If $AS^{(1\to m+1)}$ and $AS^{(m+3\to 2m+2)}$ do not make the desired equality true simultaneously, then

$$\begin{aligned} &AS^{(1\to m+1)} + AS^{(m+3\to 2m+1)} \\ &\geq (m/2)(B_d+1)+(m-2)(B_d+1)/2+1 \\ &= (m-1)(B_d+1)+1. \end{aligned}$$

Because F in the $m+2$ th round is active, we have $AS^{(m+2)} \geq B_d$ and

$$\begin{aligned} AS^{(1\to 2m+1)} &= AS^{(1\to m+1)} + AS^{(m+3\to 2m+1)} + AS^{(m+2)} \\ &\geq (m-1)(B_d+1)+1+B_d = m(B_d+1). \end{aligned}$$

This result demonstrates that (1) is true for $r = 2m+1$ when m is even. Therefore, (1) is true for $r = 2m+1$ if F in round $m+2$ is active.

Cases 1 and 2 demonstrate that (1) and (2) are true for $r = 2m+1$ if (1) and (2) are true for $r \leq 2m$.

Therefore, inductive supposition indicates that this theorem is true for $r \geq 3$.

Q.E.D.

We can obtain corresponding results for the 5-round differential characteristic in the Lai-Massey scheme with an SPS F-function according to theorem 3.

Corollary For the Lai-Massey scheme with an SPS F-function, let $B_d \geq 3$ be odd and let

$\sigma(x)=\delta(x)\oplus\sigma(0)$ be an affine orthomorphsim. Then, there are at least $2B_d+2$ active *S*-boxes in a 5-round differential characteristic, and the lower bound is reached iff the structure of the 5-round differential characteristic is

$$(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\alpha),\delta(\alpha))\to(\delta^2(\alpha),\delta(\alpha))$$
$$\to(\delta^2(\alpha),\delta^2(\alpha))\to(\delta^3(\alpha),\delta^2(\alpha))$$

for some $\alpha\neq 0$ with $Hw(\delta(\alpha)\oplus\alpha)=Hw(\delta^2(\alpha)\oplus\delta(\alpha))=(B_d+1)/2$. The corresponding differentials for F are $0\to 0$, $\delta(\alpha)\oplus\alpha\to\delta(\alpha)\oplus\alpha$, $0\to 0$, $\delta^2(\alpha)\oplus\delta(\alpha)\to\delta^2(\alpha)\oplus\delta(\alpha)$, and $0\to 0$, respectively.

Theorem 4 For the Lai-Massey scheme with an SPS *F*-function, let $B_d\geq 3$ be odd and let $\sigma(x)=\delta(x)\oplus\sigma(0)$ be an affine orthomorphism. $Y_D^{(r)}=\lfloor r/2\rfloor B_d$ is the lower bound in the corollary of lemma 2. $Low_D^{(r)}$ ($r\geq 3$) is defined as in theorem 3, then we have

$$Low_D^{(r)}-Y_D^{(r)}=\begin{cases}(r-1)/2, & if\ r\ is\ odd;\\ (r-4)/2, & if\ r\ is\ even.\end{cases}$$

Proof $Y_D^{(r)}=\lfloor r/2\rfloor B_d$ according to lemma 2; thus, according to theorem 3, we have

$$Low_D^{(r)}-Y_D^{(r)}=\begin{cases}(r-1)(B_d+1)/2-(r-1)B_d/2, & if\ r\ is\ odd;\\ (r/2-2)(B_d+1)+2B_d-rB_d/2, & if\ r\ is\ even.\end{cases}$$
$$=\begin{cases}(r-1)/2, & if\ r\ is\ odd;\\ (r-4)/2, & if\ r\ is\ even.\end{cases}$$

Q.E.D.

Theorem 3 provides the lower bound of the differentially active *S*-boxes in the Lai-Massey scheme with an SPS *F*-function, which is larger than the results obtained by the multiplication of the differential branch number and the number of active *F*-functions. Moreover, theorem 4 demonstrates that the increment has no relationship with B_d, where B_d is odd.

4. Lower Bound of Linearly Active *S*-boxes in the Lai-Massey Scheme with an SPS *F*-function

Next, we focus on the lower bound of linearly active *S*-boxes in the Lai-Massey scheme with an SPS *F*-function. Based on the duality of the structure between the differential characteristic and linear trail, the lower bound of the linearly active *S*-boxes in the Lai-Massey scheme under consideration can be easily obtained.

Theorem 5 Let $\sigma(x)=Mx\oplus C$ be affine, then the linear approximation $(\alpha,\beta)\to(A,B)$ for the round function Q has nonzero coefficient ρ iff $\alpha\oplus\beta\oplus B\oplus M^TA=0$. Besides, the linear approximation for F is $\beta\oplus B\to\alpha\oplus\beta$, and the coefficient is $\rho\times(-1)^{A\cdot C}$.

Proof See Appendix B.

Theorem 6 (The dual theorem between the differential characteristic and linear trail in the Lai-Massey scheme.)

Let σ be an affine orthomorphism. Then, the *n*-round differential characteristic $(a_{0,1},a_{0,2})\to(a_{1,1},a_{1,2})\to\cdots\to(a_{n,1},a_{n,2})$ has nonzero probability, and the corresponding differentials of F are $a_{0,1}\oplus a_{0,2}\to c_0$, $a_{1,1}\oplus a_{1,2}\to c_1$, …, $a_{n-1,1}\oplus a_{n-1,2}\to c_{n-1}$ iff $(a_{0,1},a_{0,2})\to(a_{1,1},a_{1,2})\to\cdots\to(a_{n,1},a_{n,2})$ is an *n*-round linear trail of its dual Lai-Massey scheme with a nonzero correlation coefficient and the corresponding linear approximations of the

F-function are $c_0 \to a_{0,1} \oplus a_{0,2}, c_1 \to a_{1,1} \oplus a_{1,2}, \ldots, c_{n-1} \to a_{n-1,1} \oplus a_{n-1,2}$.

Proof See Appendix C.

Based on the duality, similar results can be obtained with respect to linearly active *S*-boxes, which are stated in the following theorems 7 and 8.

Theorem 7 For the Lai-Massey scheme with an SPS *F*-function, let $B_l \geq 3$ be odd and let $\sigma(x) = Mx \oplus C$ be an affine orthomorphsim. Then, the following statements are true:

(1) There are at least $Low_L^{(r)}$ ($r \geq 3$) active *S*-boxes in an *r*-round linear trail, where

$$Low_L^{(r)} = \begin{cases} (r-1)(B_l+1)/2, & \text{if } r \text{ is odd;} \\ (r/2-2)(B_l+1)+2B_l, & \text{if } r \text{ is even.} \end{cases}$$

(2) If the number of active *S*-boxes is $Low_L^{(r)}$ in the *r*-round linear trail, then *F* is active neither in the first nor last round.

Theorem 8 For the Lai-Massey scheme with an SPS *F*-function, let $B_l \geq 3$ be odd and let $\sigma(x) = Mx \oplus C$ be an affine orthomorphsim, where $r \geq 3$. $Y_L^{(r)} = \lfloor r/2 \rfloor B_l$ is the lower bound in the corollary of lemma 2 and $Low_L^{(r)}$ is as defined as in theorem 7, then

$$Low_L^{(r)} - Y_L^{(r)} = \begin{cases} (r-1)/2, & \text{if } r \text{ is odd;} \\ (r-4)/2, & \text{if } r \text{ is even.} \end{cases}$$

For FOX64, $B_d = B_l = 5$; for FOX128, $B_d = B_l = 9$. By combining theorems 4 and 8, we can obtain the lower bound of differentially active *S*-boxes ranging from 3 rounds of FOX64 to 12 rounds of FOX64. Similarly, we can obtain the lower bound of linearly active *S*-boxes ranging from 3 rounds of FOX128 to 12 rounds of FOX128. **Table 1** compares the results of this study with those presented in [3].

Table 1. The number of active *S*-boxes in FOX64 and FOX128

Rounds(*r*)	The number of active *S*-boxes in FOX64		The number of active *S*-boxes in FOX128	
	This paper	Ref[3]	This paper	Ref[3]
3	6	5	10	9
4	10	10	18	18
5	12	10	20	18
6	16	15	28	27
7	18	15	30	27
8	22	20	38	36
9	24	20	40	36
10	28	25	48	45
11	30	25	50	45
12	34	30	58	54

The above table illustrates that the results obtained here are superior to the results in [3].

Theorem 9 It is impossible to find any useful differential of the linear characteristic after 6 rounds of FOX64.

Proof From [3], $DP_{\max}^{sbox} = LP_{\max}^{sbox} = 2^{-4}$. We can conclude that this theorem is correct from **Table 1**.

Q.E.D.

Junod and Vaudenay proved that it is impossible to find any useful differential characteristic or linear trail after 8 rounds of either FOX64 or FOX128 [3]. This paper

demonstrates that a smaller number of rounds of FOX64 can resist a differential and linear attack. For FOX128, although we do not decrease the number of rounds from 8, we obtain a more precise bound on the lower bound of the active *S*-boxes, illustrating that FOX128 is safer than previously thought.

5 Conclusions

This paper focuses on the lower bounds of differentially and linearly active *S*-boxes in a set number of consecutive rounds of the Lai-Massey scheme with an SPS *F*-function. First, we provide the lower bound of the differentially active *S*-boxes, and similar results are obtained for linearly active *S*-boxes based on the duality in the Lai-Massey scheme. Finally, we apply our results to FOX and provide a tighter bound on the lower bound of active *S*-boxes. This paper demonstrates that it is impossible to find any useful differential characteristic or linear trail after 6 rounds of FOX64, rather than the 8 rounds used by Junod and Vaudenay at SAC 2004. In addition, the corollaries in this paper have practical uses because the *P* permutations that we use in block ciphers typically have the maximum branch number, and the dimension of *P* is even, which means that the differential branch number and linear branch number of *P* are odd.

References

[1] X. Lai and J. Massey. "A proposal for a new block encryption standard," *Advances in Cryptology-EUROCRYPT'90*, *LNCS*, vol. 473, pp.389-404, 1990. Article (CrossRef Link)

[2] S.Vaudenay, "On the Lai-Massey scheme," Advances in Cryptology - *ASIACRYPT' 99*, LNCS, vol. 1716, pp. 8-19, 1999. Article (CrossRef Link)

[3] P. Junod and S.Vaudenay , "FOX: a new family of block ciphers," *SAC 2004*, LNCS, vol. 2595, pp. 131-146, Springer-Verlag, 2004. Article (CrossRef Link)

[4] Wenling Wu, Wentao Zhang and Dengguo Feng, "Integral Cryptanalysis of Reduced FOX Block Cipher," *Information Security and Cryptology - ICISC 2005*, LNCS, vol. 3935, pp. 229-241, 2006. Article (CrossRef Link)

[5] Zhongming Wu, Xuejia Lai, Bo Zhu, and Yiyuan Luo, "Impossible differential cryptanalysis of FOX," *Cryptology ePrint* /2009/357. http://eprint.iacr.org/

[6] Yuechuan Wei, Bing Sun, and Chao Li. "Impossible differential attacks on FOX," *Journal on Communications*, vol. 9, pp. 24-29, 2010. http://wenku.baidu.com/link?url=FizBvRdaVTvrwY7qKYgUvyjAMD0ZLHOQdTOhylmSTCgkSgad7xQXVTSiL_kffes0HBRCu8C3kTHQd9fk_QjJV3mg3kiJOcDto9HZ4bIAusO

[7] Wenling Wu, Hongru Wei. "Collision-integral attack of reduced-round FOX," *Journal of Electronics & Information Technology*, vol. 7, pp. 1307-1310, 2005. http://wenku.baidu.com/link?url=dpxdjBQPKYOHIGmBBEhqoMp_aD_RJj3_OF9TD1vKhoBtXVzYvoih57uRqcPx9s03YhSk-ermtAeEa26lgALGfcaz5rfkARDmvwaaGuIp7

[8] Ruilin Li, Jianxiong You, Bing Sun, et al., "Fault analysis study of the block cipher FOX64," *Multimedia Tools and Applications*, vol. 63, no. 3, pp. 691-708, 2013. Article (CrossRef Link)

[9] E.Biham and A.Shamir. "Differential cryptanalysis of DES-like cryptosystems". *Journal of Cryptology*, vol. 14, no. 1, pp. 3-72, 1991. Article (CrossRef Link)

[10] M.Matsui "Linear cryptanalysis method for DES cipher," *In Advances in Cryptology -Eurocrypt* LNCS, vol. 3788, pp. 386-397, 1993. Article (CrossRef Link)

[11] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Ohta, "A Strategy for Constructing Fast Round Functions with Practical Security against Differential and Linear Cryptanalysis," *Selected Areas in Cryptography*, LNCS, vol. 1556, pp. 264-279, 1999. Article (CrossRef Link)

[12] V. Rijmen, J. Daemon, B. Preneel, A. Bosselaers, and E. D. Win, "The cipher SHARK," *Fast*

Software Encryption — Third International Workshop, LNCS, vol.1039, pp.99–111, 1996. Article (CrossRef Link)
[13] Chenhui Jin, Haoran Zheng, Shaowu Zhang, et al.. Cryptology. *Higher Education Press*, 2009.
[14] S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon, and I. Cho. "Provable security against differential and linear cryptanalysis for the SPN structure"[C]. *FSE 2000*. LNCS, vol.1978, pp 273-283, 2001. Article (CrossRef Link)

Appendix

A Proof of Theorem 1

Theorem 1 The probability of the differential $(\alpha,\beta)\to(A,B)$ of the round function Q is nonzero iff the differentials for F and σ are $\alpha\oplus\beta\to\beta\oplus B$ and $\alpha\oplus\beta\oplus B\to A$, respectively, and the probabilities of these two differentials are both nonzero. Moreover,

$$p_Q((\alpha,\beta)\to(A,B))=p_F(\alpha\oplus\beta\to\beta\oplus B)\,p_\sigma(\alpha\oplus\beta\oplus B\to A).$$

In particular, if $\sigma(x)=\delta(x)\oplus\sigma(0)$ is affine, then the output difference of F is $\beta\oplus B=\alpha\oplus\delta^{-1}(A)$.

Proof Let the two inputs of Lai-Massey scheme be (x,y) and $(x\oplus\alpha,y\oplus\beta)$ respectively, then the outputs of F are $b_1=F(x\oplus y)$ and $b_2=F(x\oplus y\oplus\alpha\oplus\beta)$ correspondingly. Since the output difference of round function Q is

$$\begin{aligned}&Q(x\oplus\alpha,y\oplus\beta)\oplus Q(x,y)\\&=(\sigma(x\oplus\alpha\oplus F(x\oplus y\oplus\alpha\oplus\beta)),y\oplus\beta\oplus F(x\oplus y\oplus\alpha\oplus\beta))\oplus(\sigma(x\oplus F(x\oplus y)),y\oplus F(x\oplus y))\\&=(\sigma(x\oplus\alpha\oplus b_2),y\oplus\beta\oplus b_2)\oplus(\sigma(x\oplus b_1),y\oplus b_1)\\&=(\sigma(x\oplus\alpha\oplus b_2)\oplus\sigma(x\oplus b_1),\beta\oplus b_1\oplus b_2).\end{aligned}$$

Then the output difference of round function Q being (A,B) is equivalent to

$$\begin{cases}\sigma(x\oplus\alpha\oplus b_2)\oplus\sigma(x\oplus b_1)=A\\F(x\oplus y)\oplus F(x\oplus y\oplus\alpha\oplus\beta)=\beta\oplus B\end{cases},$$

which means that the differentials of F and σ are $\alpha\oplus\beta\to\beta\oplus B$ and $\alpha\oplus\beta\oplus B\to A$, respectively.

Let $z=x\oplus y$. Obviously, the number of inputs satisfying the above formula is

$$\begin{aligned}&\#\{(x,y):F(x\oplus y)\oplus F(x\oplus y\oplus\alpha\oplus\beta)=\beta\oplus B,\sigma(x\oplus\alpha\oplus b_2)\oplus\sigma(x\oplus b_1)=A\}\\&=\#\{(x,z):F(z)\oplus F(z\oplus\alpha\oplus\beta)=\beta\oplus B,\sigma(x\oplus\alpha\oplus b_2)\oplus\sigma(x\oplus b_1)=A\}\\&=\sum_z\#\{x:F(z)\oplus F(z\oplus\alpha\oplus\beta)=\beta\oplus B,\sigma(x\oplus\alpha\oplus b_2)\oplus\sigma(x\oplus b_1)=A\}\\&=\sum_{z:F(z)\oplus F(z\oplus\alpha\oplus\beta)=\beta\oplus B}\#\{x:\sigma(x\oplus\alpha\oplus b_2)\oplus\sigma(x\oplus b_1)=A\}\end{aligned}$$

Since $b_2=b_1\oplus\beta\oplus B$, then we have

$$\begin{aligned}&\sum_{z:F(z)\oplus F(z\oplus\alpha\oplus\beta)=\beta\oplus B}\#\{x:\sigma(x\oplus\alpha\oplus b_1\oplus\beta\oplus B)\oplus\sigma(x\oplus b_1)=A\}\\&=\sum_{z:F(z)\oplus F(z\oplus\alpha\oplus\beta)=\beta\oplus B}\#\{t:\sigma(t\oplus\alpha\oplus\beta\oplus B)\oplus\sigma(t)=A\}\\&=\#\{z:F(z)\oplus F(z\oplus\alpha\oplus\beta)=\beta\oplus B\}\times\#\{t:\sigma(t\oplus\alpha\oplus\beta\oplus B)\oplus\sigma(t)=A\}\end{aligned}$$

The above formula shows that the probability of the differential for round function Q is

$$p_Q((\alpha,\beta)\to(A,B))=p_F(\alpha\oplus\beta\to\beta\oplus B)\,p_\sigma(\alpha\oplus\beta\oplus B\to A).$$

So $p_Q((\alpha,\beta)\to(A,B))\neq 0$ iff $p_F(\alpha\oplus\beta\to\beta\oplus B)\neq 0$ and $p_\sigma(\alpha\oplus\beta\oplus B\to A)\neq 0$.

Specially, if σ is affine, since $p_\sigma(\alpha\oplus\beta\oplus B\to A)\neq 0$, then $p_\sigma(\alpha\oplus\beta\oplus B\to A)=1$, therefore we have $\delta(\alpha\oplus\beta\oplus B)=A$, which means that the output difference of F is $\beta\oplus B=\alpha\oplus\delta^{-1}(A)$.

B Proof of Theorem 5

Theorem 5 Let $\sigma(x)=Mx\oplus C$ be affine, then the linear approximation $(\alpha,\beta)\to(A,B)$ for the round function Q has nonzero coefficient ρ iff $\alpha\oplus\beta\oplus B\oplus M^TA=0$. Besides, the linear approximation for F is $\beta\oplus B\to\alpha\oplus\beta$, and the coefficient is $\rho\times(-1)^{A\cdot C}$.

Proof Let $(\alpha,\beta)\to(A,B)$ be the linear approximation for round function Q and its coefficient be ρ. Let (x_1,x_2) be the input of Lai-Massey scheme.

Let $x=x_1$, $y=x_1\oplus x_2$ and $F(x_1\oplus x_2)=b$, then

$$\begin{aligned}&(A,B)\cdot Q_k(x_1,x_2)\oplus(\alpha,\beta)\cdot(x_1,x_2)\\ =&A\cdot\sigma(F(x_1\oplus x_2)\oplus x_1)\oplus B\cdot(F(x_1\oplus x_2)\oplus x_2)\oplus\alpha\cdot x_1\oplus\beta\cdot x_2\\ =&\alpha\cdot x\oplus A\cdot\sigma(x)\oplus(\beta\oplus B)\cdot(x\oplus y)\oplus A\cdot\sigma(F(y))\oplus B\cdot F(y)\oplus A\cdot C\\ =&(\alpha\oplus\beta\oplus B)\cdot x\oplus A\cdot\sigma(x)\oplus(\beta\oplus B)\cdot y\oplus A\cdot\sigma(F(y))\oplus B\cdot F(y)\oplus A\cdot C\end{aligned}$$

Let all the variables be row vectors. From $\sigma(x)=Mx\oplus C$, we can get

$$\begin{aligned}&(\alpha\oplus\beta\oplus B)\cdot x\oplus A\cdot Mx\oplus A\cdot C\oplus(\beta\oplus B)\cdot y\oplus A\cdot MF(y)\oplus B\cdot F(y)\oplus A\cdot C\oplus A\cdot C\\ =&(\alpha\oplus\beta\oplus B)^Tx\oplus A^TMx\oplus(\beta\oplus B)^Ty\oplus A^TMF(y)\oplus B^TF(y)\oplus A\cdot C\\ =&[(\alpha\oplus\beta\oplus B)^T\oplus A^TM]x\oplus(A^TM\oplus B^T)F(y)\oplus(\beta\oplus B)^Ty\oplus A\cdot C\\ =&(\alpha\oplus\beta\oplus B\oplus M^TA)\cdot x\oplus(M^TA\oplus B)\cdot F(y)\oplus(\beta\oplus B)\cdot y\oplus A\cdot C\end{aligned}$$

Therefore , we get

$$\begin{aligned}&\sum_{x_1,x_2}(-1)^{(A,B)\cdot Q_k(x_1,x_2)\oplus(\alpha,\beta)\cdot(x_1,x_2)}=\sum_{x,y}(-1)^{(\alpha\oplus\beta\oplus B\oplus M^TA)\cdot x\oplus(M^TA\oplus B)\cdot F(y)\oplus(\beta\oplus B)\cdot y\oplus A\cdot C}\\ =&[\sum_x(-1)^{(\alpha\oplus\beta\oplus B\oplus M^TA)\cdot x}][\sum_y(-1)^{(M^TA\oplus B)\cdot F(y)\oplus(\beta\oplus B)\cdot y\oplus A\cdot C}].\end{aligned}$$

If $\alpha\oplus\beta\oplus B\oplus M^TA\neq0$, then $\sum_x(-1)^{(\alpha\oplus\beta\oplus B\oplus M^TA)\cdot x}=0$, thus

$$\sum_{x_1,x_2}(-1)^{(A,B)\cdot Q_k(x_1,x_2)\oplus(\alpha,\beta)\cdot(x_1,x_2)}=0.$$

This is a contradiction to $\rho\neq0$, so

$$\begin{aligned}W_{(Q_k)}((\alpha,\beta)\to(A,B))&=W_{(F)}(\beta\oplus B\to M^TA\oplus B)\times(-1)^{A\cdot C}\\ &=W_{(F)}(\beta\oplus B\to\alpha\oplus\beta)\times(-1)^{A\cdot C},\end{aligned}$$

which proves this theorem.

C Proof of Theorem 6

First, we give the relationship between the structure of the differential and the linear approximation in Lai-Massey scheme.

Lemma 3 Let σ be affine and bijective, then the differential with nonzero probability of round function is $(\alpha_0,\alpha_1)\to(\beta_0,\beta_1)$ and the corresponding differential for F is $\alpha_0\oplus\alpha_1\to c$ iff the round function of its dual Lai-Massey scheme has linear approximation $(\alpha_0,\alpha_1)\to(\beta_0,\beta_1)$ with nonzero coefficient, and the corresponding linear approximation for F is $c\to\alpha_0\oplus\alpha_1$.

Proof By theorem 1, the probability of the differential $(\alpha_0,\alpha_1)\to(\beta_0,\beta_1)$ for the round function is nonzero iff the differential for F is $\alpha_0\oplus\alpha_1\to\alpha_1\oplus\beta_1$, and $\alpha_0\oplus\alpha_1\oplus\beta_1=M^{-1}\beta_0$.

From theorem 5 we know that the round function of its dual Lai-Massey scheme has linear approximation $(\alpha_0,\alpha_1)\to(\beta_0,\beta_1)$ with nonzero coefficient iff the linear approximation for F is $\alpha_1\oplus\beta_1\to\alpha_0\oplus\alpha_1$, and $\alpha_0\oplus\alpha_1\oplus\beta_1\oplus((M^{-1})^T)^T\beta_0=0$, i.e., $\alpha_0\oplus\alpha_1\oplus\beta_1=M^{-1}\beta_0$, so this theorem is true.

Theorem 6 (The dual theorem between differential characteristic and linear trail of Lai-Massey

scheme)

Let σ be affine and bijective, then the n-round differential characteristic $(a_{0,1}, a_{0,2}) \to (a_{1,1}, a_{1,2}) \to \cdots \to (a_{n,1}, a_{n,2})$ has nonzero probability and the corresponding differentials for F are $a_{0,1} \oplus a_{0,2} \to c_0$, $a_{1,1} \oplus a_{1,2} \to c_1$,…, $a_{n-1,1} \oplus a_{n-1,2} \to c_{n-1}$ iff $(a_{0,1}, a_{0,2}) \to (a_{1,1}, a_{1,2}) \to \cdots \to (a_{n,1}, a_{n,2})$ is an n-round linear trail of its dual Lai-Massey scheme with nonzero coefficient and the corresponding linear approximations for F are $c_0 \to a_{0,1} \oplus a_{0,2}$, $c_1 \to a_{1,1} \oplus a_{1,2}$,…, $c_{n-1} \to a_{n-1,1} \oplus a_{n-1,2}$ respectively.

Proof This theorem can be obtained through inductive assumption by using lemma 3 above.

Lishi Fu was born in 1989. She is currently pursuing for the Ph.D degree in the Information Science and Technology Institute. Her current research interest is the analysis of block cipher.
E-mail: fulishi123@sohu.com

Chenhui Jin was born in 1965. Currently, he is a professor in the Information Science and Technology Institute. His current research interests are cryptography and information security.
E-mail: jinchenhui @126.com