SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

December 2017, Vol. 60 122101:1–122101:9
doi: 10.1007/s11432-016-0477-8

Revised cryptanalysis for SMS4

Lei CHENG[1,2], Bing SUN[1,2,3] & Chao LI[1*]

[1]*College of Science, National University of Defense Technology, Changsha* 410073*, China;*
[2]*State Key Laboratory of Cryptology, P.O. Box* 5159*, Beijing* 100878*, China;*
[3]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China*

Received July 12, 2016; accepted September 8, 2016; published online March 13, 2017

Abstract SMS4 is released by the Chinese government as part of the WAPI standard for the wireless networks. At ICICS 2007 and CRYPTO 2015, Lu and Sun et al. constructed some 12-round impossible differentials and 12-round zero correlation linear hulls, respectively. In this paper, it is proved that the distinguishers constructed by Lu and Sun et al. are independent with the details of the non-linear layers though they concentrated on the specific S-boxes. This indicates that for the structure deduced by SMS4, there always exist 12-round impossible differentials and 12-round zero correlation linear hulls.

Keywords SMS4, impossible differential, zero correlation linear hull, structure, integral

Citation Cheng L, Sun B, Li C. Revised cryptanalysis for SMS4. Sci China Inf Sci, 2017, 60(12): 122101, doi: 10.1007/s11432-016-0477-8

1 Introduction

With the development of networks and communications, cryptography has been a useful approach for security protection. As a major primitive in the field of symmetric cryptography, block cipher has attracted more attention in recent years, due to the high security as well as efficient implementation. SMS4[1)] block cipher was released by the Chinese government in January 2006, which was designed for the WAPI (Wired Authentication and Privacy Infrastructure) standard, and WAPI is officially mandated for securing wireless networks within China. Since its publication, SMS4 has been the target of many cryptanalyses such as differential cryptanalysis [1–3], linear cryptanalysis [4, 5], impossible differential cryptanalysis [6, 7], zero correlation linear cryptanalysis [8], integral cryptanalysis [8–10] and algebraic cryptanalysis [11, 12].

Impossible differential cryptanalysis was independently proposed by Knudsen [13] and Biham [14], which uses the differentials with probability 0 to discard the wrong keys. The common method is the miss-in-the-middle technique [15] to construct the impossible differentials of some round-reduced ciphers. Generally, it is difficult to guarantee completeness in a search for impossible differentials. Therefore, from the practical point of view, we are more interested in the impossible differentials that are independent of

* Corresponding author (email: academic_lc@163.com)

1) Specification of SMS4, block cipher for WLAN products—SMS4 (in Chinese). http://www.oscca.gov.cn/UpFile/2006 21016423197990.pdf.

the S-boxes. Some automatic tools for searching impossible differentials of a cipher have been exploited in [16–18]. So far, the longest impossible differential of SMS4 which was found by Lu at ICICS 2007 [6] covers 12 rounds.

Property 1 ([6]). For any nonempty subset Λ of $\{0, 1, \ldots, 15\}$, let e_Λ be a 32-bit word with zeros at all positions except the ones in Λ. Then

$$(e_\Lambda, e_\Lambda, e_\Lambda, 0) \to (0, e_\Lambda, e_\Lambda, e_\Lambda)$$

is a 12-round impossible differential of SMS4.

Assume that the input difference is $(\alpha, \alpha, \alpha, 0)$ where α is some specific value, then the output difference of the sixth-round belongs to some subset $D_\alpha^{(e)}$ which can be constructed based on the difference distribution table of the S-box. Assume that the output difference of the twelfth round is $(0, \alpha, \alpha, \alpha)$, then the input difference of the seventh-round belongs to some subset $D_\alpha^{(d)}$. If $D_\alpha^{(e)} \cap D_\alpha^{(d)} = \emptyset$, an impossible differential is constructed. However, due to the computing limitation, Lu can only apply a partially exhaustive searching for such α.

Zero correlation linear cryptanalysis, proposed by Bogdanov and Rijmen in [19], tries to construct some linear hulls with correlation exactly zero. The procedure of constructing zero correlation linear hulls of a cipher is similar to the procedure of constructing impossible differentials. By using the linear distribution table of the S-box, Sun et al. built some zero correlation linear hulls of 12-round SMS4 [8]:

Property 2 ([8]). Let $V = \{v \in (\mathbb{F}_2^8)^4 | HW(\mathcal{L}^{\mathrm{T}} v) = 1\}$, where $HW(x_1, x_2, x_3, x_4) = \#\{x_i \neq 0, i = 1, 2, 3, 4\}$ and $\mathcal{L}^{\mathrm{T}}$ is the transposition of the linear layer of the round function. For any $d \in V$, $(0, 0, 0, d) \to (d, 0, 0, 0)$ is a 12-round zero correlation linear hull of SMS4.

Integral cryptanalysis, which was proposed by Knudsen, is one of the most important cryptanalytic methods [20,21]. According to the link between zero correlation linear hulls and integral distinguishers [8], we can deduce an integral distinguisher of 12-round SMS4 based on the 12-round zero correlation linear hulls.

In this paper, we prove that 12-round distinguishers given by Lu and Sun et al. are irrelevant to the S-boxes. Even if we choose some other S-boxes in SMS4, these impossible differentials and zero correlation linear hulls still remain the same.

Main contributions. We further investigate the known distinguishers and obtain the following results.

(1) The impossible differentials of 12-round SMS4 constructed at ICICS 2007 are independent with the S-boxes;

(2) The zero correlation linear hulls of 12-round SMS4 presented at CRYPTO 2015 are also independent with the S-boxes.

Organization of the paper. The remainder of this paper is organized as follows. Section 2 introduces the notations and concepts that will be used throughout the paper. In Sections 3 and 4, we are going to present the revised impossible differential and zero correlation linear cryptanalysis for SMS4. Finally, Section 5 concludes this paper.

2 Preliminaries

Let $\mathbb{F}_2$ denote the finite fields with two elements, and $\mathbb{F}_2^n$ be the vector space over $\mathbb{F}_2$ with dimension n.

2.1 Impossible differential

Let $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathbb{F}_2^n$. Then

$$a \cdot b \triangleq a_1 b_1 \oplus \cdots \oplus a_n b_n$$

denotes the inner product of a and b. Given a vectorial function $H : \mathbb{F}_2^n \to \mathbb{F}_2^k$, the correlation of the linear approximation for a k-bit output mask b and an n-bit input mask a is defined by

$$c(a \xrightarrow{H} b) \triangleq \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot H(x)}.$$

If $c(a \xrightarrow{H} b) = 0$, then $a \xrightarrow{H} b$ is called a zero correlation linear hull of H [19].

Let $\delta \in \mathbb{F}_2^n$ and $\Delta \in \mathbb{F}_2^k$. The differential probability for an input difference δ and an output difference Δ is defined as

$$p(\delta \xrightarrow{H} \Delta) \triangleq \frac{\#\{x \in \mathbb{F}_2^n | H(x) \oplus H(x \oplus \delta) = \Delta\}}{2^n}.$$

If $p(\delta \xrightarrow{H} \Delta) = 0$, then $\delta \xrightarrow{H} \Delta$ is called an impossible differential of H [13,14].

Assume $x = (x_1, x_2, x_3, x_4) \in (\mathbb{F}_2^8)^4$. The support of $x = (x_1, x_2, x_3, x_4) \in (\mathbb{F}_2^8)^4$ is defined as

$$\mathrm{supp}(x) = \{i | x_i \neq 0, i = 1, 2, 3, 4\}.$$

And the Hamming weight of $x = (x_1, x_2, x_3, x_4) \in (\mathbb{F}_2^8)^4$ is defined as

$$H_w(x) = \#\mathrm{supp}(x),$$

i.e., the Hamming weight of x is the number of non-zero components of x.

2.2 The SMS4 cipher

The SMS4 cipher has a 128-bit block size, a 128-bit user key and a total of 32 rounds. The 128-bit plaintext P is divided into four 32-bit words $P = (P_1, P_2, P_3, P_4)$. Let $M_{i+1} = (M_{i+1,1}, M_{i+1,2}, M_{i+1,3}, M_{i+1,4})$ denote the four 32-bit output of the i-th round ($1 \leqslant i \leqslant 32$). The encryption of SMS4 can be described as follows.

(1) Set $M_1 = (M_{1,1}, M_{1,2}, M_{1,3}, M_{1,4}) = (P_1, P_2, P_3, P_4)$.

(2) For $i = 1$ to 32, $M_{i+1,1} = M_{i,2}, M_{i+1,2} = M_{i,3}, M_{i+1,3} = M_{i,4}, M_{i+1,4} = M_{i,1} \oplus F(M_{i+1,1} \oplus M_{i+1,2} \oplus M_{i+1,3} \oplus RK_i)$, where the RK_i is the i-th round key and $F : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$ is the round function, which is defined as follows (see Figure 1).

Assume that $N = (N_1, N_2, N_3, N_4) \in (\mathbb{F}_2^8)^4$, S be an 8×8 bijective S-box and $N \lll_i$ be left rotation of N by i bits. Let

$$\mathcal{S}(N) = (S(N_1), S(N_2), S(N_3), S(N_4)),$$

and

$$\mathcal{L}(N) = N \oplus (N \lll_2) \oplus (N \lll_{10}) \oplus (N \lll_{18}) \oplus (N \lll_{24}).$$

Then $F(N) = \mathcal{L} \circ \mathcal{S}(N)$.

(3) The cipher-text is defined as

$$C = (C_1, C_2, C_3, C_4) = (M_{33,1}, M_{33,2}, M_{33,3}, M_{33,4}).$$

We do not exploit the key schedule and the specific of the S-box throughout this paper. In this paper, $\mathcal{L}$ is also regarded as an $\mathbb{F}_2^{32} \times \mathbb{F}_2^{32}$ matrix. $\mathcal{L}^{\mathrm{T}}$ denote the matrix transposition of $\mathcal{L}$, which is used in Section 4. Then $\mathcal{L}^{\mathrm{T}}$ is also a linear function on $\mathbb{F}_2^{32}$.

3 Revised impossible differential cryptanalysis for SMS4

At ICICS 2007, based on the difference distribution table (DDT) of the S-box, Lu tried to find some α, so that

$$(\alpha, \alpha, \alpha, 0) \to (0, \alpha, \alpha, \alpha)$$

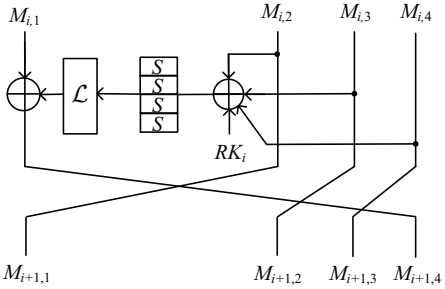

Figure 1 Round Function of SMS4.

is an impossible differential of 12-round SMS4. Due to the limitation of computing capacity, he can only exhaustive α with the form $(0, 0, \alpha_2, \alpha_3)$ where (α_2, α_3) is an arbitrary nonzero element in $\mathbb{F}_2^8 \times \mathbb{F}_2^8$. In this section, we will prove that these impossible differentials are irrelevant to the details of the S-boxes, i.e., we can build these distinguishers without using the difference distribution table of the S-box.

Assume that F is a permutation on $\mathbb{F}_2^{32}$. For any $\alpha \in \mathbb{F}_2^{32}$, let

$$\mathcal{D}_F(\alpha) = \left\{ \beta \in \mathbb{F}_2^{32} \middle| p\left(\alpha \xrightarrow{F} \beta\right) > 0 \right\}.$$

Thus for $\beta \in \mathbb{F}_2^{32}$, $p(\alpha \xrightarrow{F} \beta) > 0$ if and only if $\beta \in \mathcal{D}_F(\alpha)$. Since F is a permutation, we have Lemma 1.

Lemma 1. $0 \in \mathcal{D}_F(\alpha)$ if and only if $\alpha = 0$.

Lemma 1 indicates that for permutations, a non-zero input difference can only lead to a non-zero output difference. Now, we are going to prove the following theorem.

Theorem 1. The impossible differentials of 12-round SMS4 presented at ICICS 2007 (Property 1 in this paper) are independent with the details of the S-boxes.

Proof. See Figure 2. Suppose the input difference of SMS4 is $(\alpha, \alpha, \alpha, 0)$, $\alpha \neq 0$. In order to construct a possible differential characteristic, the output difference of the 1st, 2nd and 3rd round should be $(\alpha, \alpha, 0, \alpha)$, $(\alpha, 0, \alpha, \alpha)$ and $(0, \alpha, \alpha, \alpha)$ respectively.

Then the output difference of the 4th and 5th rounds are $(\alpha, \alpha, \alpha, a_1)$ and $(\alpha, \alpha, a_1, \alpha \oplus a_2)$ respectively, where $a_1 \in \mathcal{D}_F(\alpha)$ and $a_2 \in \mathcal{D}_F(a_1)$. Therefore, the output difference of the 6th round is

$$(\alpha, a_1, \alpha \oplus a_2, \alpha \oplus a_3),$$

where $a_3 \in \mathcal{D}_F(a_1 \oplus a_2)$.

Similarly, let the output difference of the 12th round be $(0, \alpha, \alpha, \alpha)$. The output difference of the 8th and 7th round are $(b_1, \alpha, \alpha, \alpha)$ and $(\alpha \oplus b_2, b_1, \alpha, \alpha)$, respectively, where $b_1 \in \mathcal{D}_F(\alpha)$ and $b_2 \in \mathcal{D}_F(b_1)$. Finally, the output difference of the 6th round is

$$(\alpha \oplus b_3, \alpha \oplus b_2, b_1, \alpha),$$

where $b_3 \in \mathcal{D}_F(b_1 \oplus b_2)$. Therefore, we have

$$\begin{cases} \alpha = \alpha \oplus b_3, \\ a_1 = \alpha \oplus b_2, \\ \alpha \oplus a_2 = b_1, \\ \alpha \oplus a_3 = \alpha, \end{cases}$$

which indicates that $a_3 = b_3 = 0$ and $a_1 \oplus b_2 = a_2 \oplus b_1 = \alpha$.

Taking the fact that $a_3 \in \mathcal{D}_{\mathcal{L}\circ\mathcal{S}}(a_1 \oplus a_2)$ and $b_3 \in \mathcal{D}_{\mathcal{L}\circ\mathcal{S}}(b_1 \oplus b_2)$ into consideration, we can get that

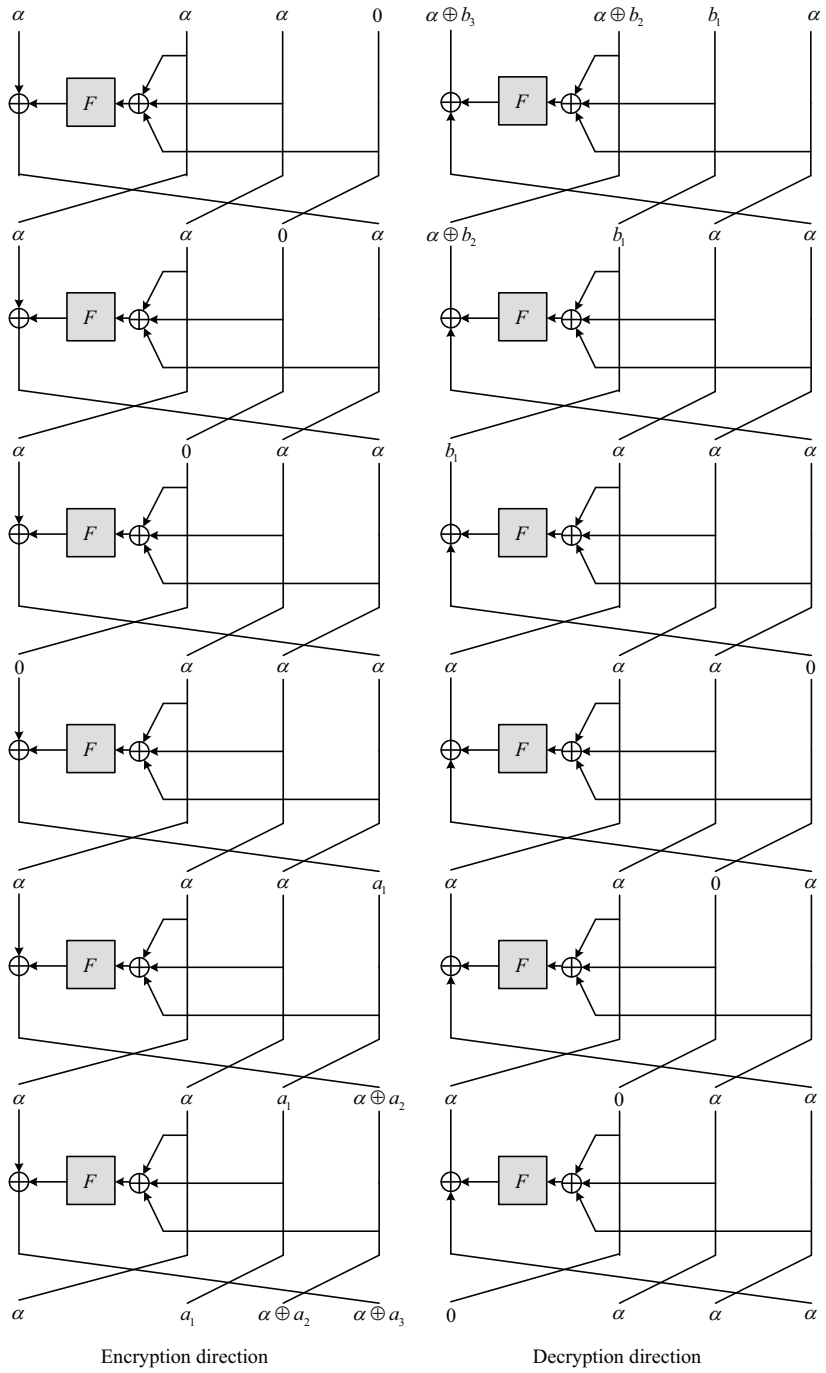

Figure 2 12-Round impossible differential of SMS4.

$a_1 \oplus a_2 = 0$ and $b_1 \oplus b_2 = 0$. Thus,

$$\begin{cases} a_1 \oplus b_1 = \alpha, \\ a_1 \in \mathcal{D}_{\mathcal{L}\circ\mathcal{S}}(\alpha), \\ b_1 \in \mathcal{D}_{\mathcal{L}\circ\mathcal{S}}(\alpha), \\ a_1 = a_2 \in \mathcal{D}_{\mathcal{L}\circ\mathcal{S}}(a_1), \\ b_1 = b_2 \in \mathcal{D}_{\mathcal{L}\circ\mathcal{S}}(b_1). \end{cases} \tag{1}$$

Accordingly, if $(\alpha, \alpha, \alpha, 0) \to (0, \alpha, \alpha, \alpha)$ is a possible differential for 12-round SMS4, there always exist a_1 and b_1 such that system (1) holds.

It follows from $a_1 \in \mathcal{D}_{\mathcal{L}\circ\mathcal{S}}(\alpha)$ and $b_1 \in \mathcal{D}_{\mathcal{L}\circ\mathcal{S}}(\alpha)$ that

$$\begin{cases}\mathcal{L}^{-1}(a_1) \in \mathcal{D}_{\mathcal{S}}(\alpha),\\ \mathcal{L}^{-1}(b_1) \in \mathcal{D}_{\mathcal{S}}(\alpha),\end{cases}$$

therefore $\mathrm{supp}(\mathcal{L}^{-1}(a_1)) = \mathrm{supp}(\mathcal{L}^{-1}(b_1)) = \mathrm{supp}(\alpha)$.

Note that $\mathcal{L}^{-1}(a_1) \oplus \mathcal{L}^{-1}(b_1) = \mathcal{L}^{-1}(\alpha)$, we can obtain

$$\mathrm{supp}(\mathcal{L}^{-1}(\alpha)) = \mathrm{supp}(\mathcal{L}^{-1}(a_1) \oplus \mathcal{L}^{-1}(b_1)) \subseteq \mathrm{supp}(\alpha). \tag{2}$$

Thus,

$$\#\mathrm{supp}(\mathcal{L}^{-1}(\alpha)) \leqslant \#\mathrm{supp}(\alpha) = \#\mathrm{supp}((0,0,*,*)) \leqslant 2,$$

where $*$ is an arbitrary value in $\mathbb{F}_2^8$.

However, for any $\alpha \neq 0$, the differential branch number of $\mathcal{L}$ being 5 means that

$$H_w(\alpha) + H_w(\mathcal{L}^{-1}(\alpha)) = \#\mathrm{supp}(\alpha) + \#\mathrm{supp}(\mathcal{L}^{-1}(\alpha)) \geqslant 5,$$

which is a contradiction.

To characterize what "being independent with the details of the S-boxes" means that for a block cipher E, Sun et al. proposed the concept of the structure $\mathcal{E}^E$, which is deduced by E: $\mathcal{E}^E$ is a set of all the ciphers that keep the linear parts of E. Generally, according to the formula (2) in the proof of Theorem 1, we have the following corollary.

Corollary 1. $(\alpha,\alpha,\alpha,0) \to (0,\alpha,\alpha,\alpha)$ is always a 12-round impossible differential of the structure $\mathcal{E}^{\mathrm{SMS4}}$ deduced by SMS4 if $\mathrm{supp}(\mathcal{L}^{-1}(\alpha))$ is not a subset of $\mathrm{supp}(\alpha)$.

4 Revised zero correlation linear cryptanalysis for SMS4

At CRYPTO 2015, based on the method of building impossible differentials for SMS4, Sun et al. found that

$$(0,0,0,\alpha) \to (\alpha,0,0,0)$$

is a zero correlation linear hull of 12-round SMS4, when $H_w(\mathcal{L}^{\mathrm{T}}(\alpha)) = 1$ and $\alpha \in \mathbb{F}_2^{32}$. Using the link between the zero correlation linear hull and integral distinguisher, they obtained a corresponding integral distinguisher for 12-round SMS4.

Assume that F is a permutation on $\mathbb{F}_2^{32}$. For any $\alpha \in \mathbb{F}_2^{32}$, let

$$\mathcal{V}_F(\alpha) = \left\{\beta \in \mathbb{F}_2^{32} \middle| c\left(\beta \xrightarrow{F} \alpha\right) \neq 0\right\}.$$

Then for $\beta \in \mathbb{F}_2^{32}$, $c(\beta \xrightarrow{F} \alpha) \neq 0$ if and only if $\beta \in \mathcal{V}_F(\alpha)$. Since F is a permutation, we have Lemma 2.

Lemma 2. $0 \in \mathcal{V}_F(\alpha)$ if and only if $\alpha = 0$.

In parallel with the proof of Theorem 1, we obtain the following theorem.

Theorem 2. The zero correlation linear hulls of 12-round SMS4 presented at CRYPTO 2015 (Property 2 in this paper) are independent with the details of the S-boxes.

Proof. As showed in Figure 3, let the input mask of SMS4 be $(0,0,0,\alpha)$. Then to build a characteristic with non-zero correlation, the output mask of the 6th round is

$$(a_1 \oplus a_2 \oplus a_3, \alpha \oplus a_2 \oplus a_3, a_1 \oplus a_3, a_1 \oplus a_2),$$

where $a_1 \in \mathcal{V}_F(\alpha)$, $a_2 \in \mathcal{V}_F(a_1)$ and $a_3 \in \mathcal{V}_F(a_1 \oplus a_2)$.

From the decryption direction, if the output mask of the 12th round is $(\alpha,0,0,0)$, the output mask of the 6th round will be

$$(b_1 \oplus b_2, b_1 \oplus b_3, \alpha \oplus b_2 \oplus b_3, b_1 \oplus b_2 \oplus b_3),$$

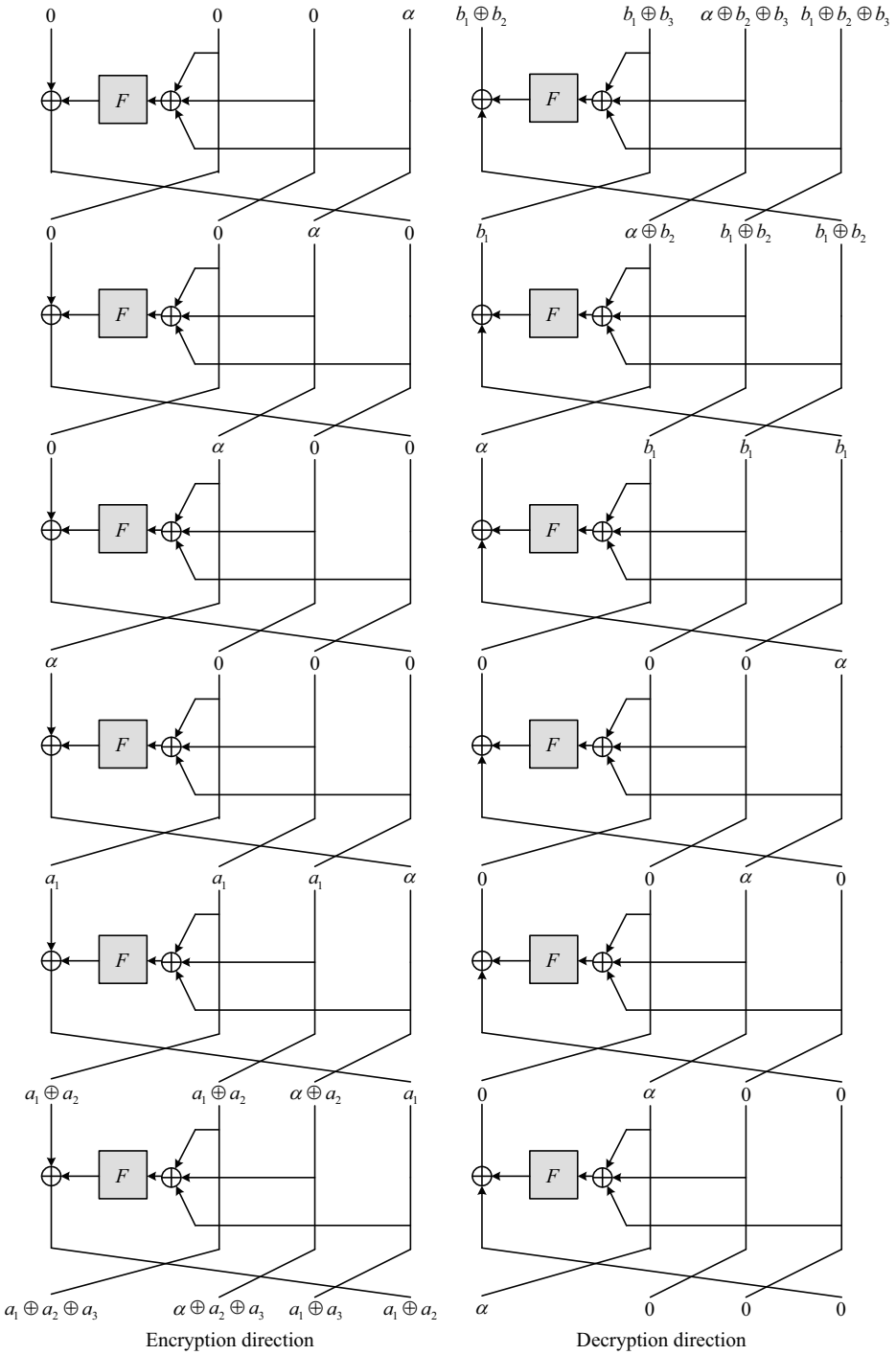

Figure 3 12-Round zero correlation linear hull of SMS4.

where $b_1 \in \mathcal{V}_F(\alpha)$, $b_2 \in \mathcal{V}_F(b_1)$ and $b_3 \in \mathcal{V}_F(b_1 \oplus b_2)$. Thus, we obtain the following system:

$$\begin{cases} a_1 \oplus a_2 \oplus a_3 = b_1 \oplus b_2, \\ \alpha \oplus a_2 \oplus a_3 = b_1 \oplus b_3, \\ a_1 \oplus a_3 = \alpha \oplus b_2 \oplus b_3, \\ a_1 \oplus a_2 = b_1 \oplus b_2 \oplus b_3, \end{cases}$$

which results in $a_3 = b_3 = 0$ and $a_1 \oplus b_2 = a_2 \oplus b_1 = \alpha$.

Since $a_3 \in \mathcal{V}_{\mathcal{L}\circ\mathcal{S}}(a_1 \oplus a_2)$ and $b_3 \in \mathcal{V}_{\mathcal{L}\circ\mathcal{S}}(b_1 \oplus b_2)$, both $a_1 \oplus a_2$ and $b_1 \oplus b_2$ are 0, which implies that

$$\begin{cases} a_1 \oplus b_1 = \alpha, \\ a_1 \in \mathcal{V}_{\mathcal{L}\circ\mathcal{S}}(\alpha), \\ b_1 \in \mathcal{V}_{\mathcal{L}\circ\mathcal{S}}(\alpha), \\ a_1 = a_2 \in \mathcal{V}_{\mathcal{L}\circ\mathcal{S}}(a_1), \\ b_1 = b_2 \in \mathcal{V}_{\mathcal{L}\circ\mathcal{S}}(b_1). \end{cases} \tag{3}$$

If $(0,0,0,\alpha) \to (\alpha,0,0,0)$ is a 12-round non-zero correlation linear hull of SMS4, we can always find some a_1 and b_1 such that system (3) holds.

It follows from $a_1 \in \mathcal{V}_{\mathcal{L}\circ\mathcal{S}}(\alpha)$ and $b_1 \in \mathcal{V}_{\mathcal{L}\circ\mathcal{S}}(\alpha)$ that

$$\begin{cases} a_1 \in \mathcal{V}_{\mathcal{S}}(\mathcal{L}^{\mathrm{T}}(\alpha)), \\ b_1 \in \mathcal{V}_{\mathcal{S}}(\mathcal{L}^{\mathrm{T}}(\alpha)), \end{cases}$$

thus $\mathrm{supp}(a_1) = \mathrm{supp}(b_1) = \mathrm{supp}(\mathcal{L}^{\mathrm{T}}(\alpha))$.

As $a_1 \oplus b_1 = \alpha$, we have

$$\mathrm{supp}(\alpha) = \mathrm{supp}(a_1 \oplus b_1) \subseteq \mathrm{supp}(a_1) \cup \mathrm{supp}(b_1) = \mathrm{supp}(\mathcal{L}^{\mathrm{T}}(\alpha)). \tag{4}$$

Therefore, $\#\mathrm{supp}(\alpha) \leqslant \#\mathrm{supp}(\mathcal{L}^{\mathrm{T}}(\alpha)) = H_w(\mathcal{L}^{\mathrm{T}}(\alpha)) = 1$. Hence $\alpha \neq 0$ indicates $H_w(\alpha) = 1$ and $H_w(\alpha) + H_w(\mathcal{L}^{\mathrm{T}}(\alpha)) = 2$.

On the other hand, the linear branch number of $\mathcal{L}$ being 5 means that $H_w(\alpha) + H_w(\mathcal{L}^{\mathrm{T}}(\alpha)) \geqslant 5$ for any $\alpha \neq 0$ which is a contradiction.

Hence $(0,0,0,\alpha) \to (\alpha,0,0,0)$ is a 12-round zero correlation linear hull of SMS4 if $H_w(\mathcal{L}^{\mathrm{T}}(\alpha)) = 1$.

Similarly, Theorem 2 can be extended to more general cases on the basis of the formula (4).

Corollary 2. $(0,0,0,\alpha) \to (\alpha,0,0,0)$ is always a 12-round zero correlation linear hull of $\mathcal{E}^{\mathrm{SMS4}}$ deduced by SMS4 if $\mathrm{supp}(\alpha)$ is not a subset of $\mathrm{supp}(\mathcal{L}^{\mathrm{T}}(\alpha))$.

Based on the link between the zero correlation linear and integral distinguishers, these integral distinguishers presented at CRYPTO 2015 are indeed irrelevant to the details of the S-boxes. Therefore, there exist 12-round integral distinguishers of $\mathcal{E}^{\mathrm{SMS4}}$.

Furthermore, the methods presented by Lu and Sun et al. are also used in this paper to demonstrate how the details of the S-boxes will infect the 12-round impossible differentials and zero correlation linear hulls of SMS4. We can both search 519706 αs through the method deduced by Sun et al. and the method deduced by Corollary 2 when 0x57000000$\leqslant \alpha \leqslant$ 0x58FFFFFF where 0x denotes the hexadecimal number. It is surprised to find that for random S-boxes, what we has found are exactly the same as Corollarys 1 and 2 on a small scale. Therefore we have the following conjecture.

Conjecture. Corollarys 1 and 2 have given all the impossible differentials and zero correlation linear hulls of 12-round $\mathcal{E}^{\mathrm{SMS4}}$.

5 Conclusion

This paper mainly focused on the impossible differentials and zero correlation linear hulls of SMS4 which was released by the Chinese government. Constructing impossible differentials and zero correlation linear hulls of block ciphers is one of the main task of the security evaluations of cryptographic schemes. Up to now, for ciphers which use S-boxes as the non-linear components, most methods do not investigate the details of S-boxes to build these two kinds of distinguishers. Refs. [6, 8] tried to exploit the specific S-boxes to construct impossible differentials and zero correlation linear hulls of SMS4 respectively.

We proved in this paper that the 12-round impossible differentials and 12-round zero correlation linear hulls not only hold for SMS4 but also hold for the structure $\mathcal{E}^{\mathrm{SMS4}}$ deduced by SMS4. Namely, although

Lu and Sun et al. used the details of the S-boxes to construct these distinguishers, these impossible differentials and zero correlation linear hulls are indeed independent with the details of the S-boxes.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61672530, 61402515), and Research Fund for the Doctoral Program of Higher Education of China (Grant No. 2012150112004)

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Zhang L, Zhang W T, Wu W L. Cryptanalysis of reduced-round SMS4 block cipher. In: Proceedings of the 13th Australasian Conference on Information Security and Privacy, Wollongong, 2008. 216–229
2 Zhang W T, Wu W L, Feng D G, et al. Some new observations on the SMS4 block cipher in the Chinese WAPI standard. In: Proceedings of the 5th International Conference on Information Security Practice and Experience, Xi'an, 2009. 324–335
3 Su B Z, Wu W L, Zhang W T. Security of the SMS4 block cipher against differential cryptanalysis. J Comput Sci Tech, 2011, 26: 130–138
4 Etrog J, Robshaw M J. The cryptanalysis of reduced-round SMS4. In: Selected Areas in Cryptography. Berlin: Springer, 2009. 51–65
5 Liu Z Q, Gu D W, Zhang J. Multiple linear cryptanalysis of reduced-round SMS4 block ciphers. Chinese J Electron, 2010, 19: 389–393
6 Lu J Q. Attacking reduced-round versions of the SMS4 block cipher in the Chinese WAPI standard. In: Proceedings of the 9th International Conference on Information and Communications Security, Zhengzhou, 2007. 306–318
7 Toz D, Dunkelman O. Analysis of two attacks on reduced-round versions of the SMS4. In: Proceedings of the 10th International Conference on Information and Communications Security, Birmingham, 2008. 141–156
8 Sun B, Liu Z Q, Rijmen V, et al. Links among impossible differential, integral and zero correlation linear cryptanalysis. In: Advances in Cryptology — CRYPTO 2015. Berlin: Springer. 2015. 95–115
9 Zhang W T, Su B Z, Wu W L, et al. Extending higher-order integral: an efficient unified algorithm of constructing integral distinguishers for block ciphers. In: Applied Cryptography and Network Security. Berlin: Springer, 2012. 117–134
10 Liu F, Ji W, Hu L, et al. Analysis of the SMS4 block cipher. In: Information Security and Privacy. Berlin: Springer, 2007. 158–170
11 Erickson J, Ding J T, Christensen C. Algebraic cryptanalysis of SMS4: Gröbner basis attack and SAT attack compared. In: Proceedings of the 12th International Conference on Information, Security and Cryptology, Seoul, 2009. 73–86
12 Ji W, Hu L. New description of SMS4 by an embedding over $GF(2^8)$. In: Proceedings of the 8th International Conference on Progress in Cryptology, Chennai, 2007. 238–251
13 Knudsen L R. DEAL – A 128-bit Block Cipher. Technical Report, Department of Informatics, University of Bergen, Norway, 1998
14 Biham E, Biryukov A, Shamir A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques, Prague, 1999. 12–23
15 Biham E, Biryukov A, Shamir A. Miss in the middle attacks on IDEA and Khufu. In: Proceedings of the 6th International Workshop on Fast Software Encryption. London: Springer, 1999. 124–138
16 Kim J, Hong S, Sung J, et al. Impossible differential cryptanalysis for block cipher structures. In: Progress in Cryptology — INDOCRYPT. Berlin: Springer, 2003. 82–96
17 Luo Y Y, Lai X J, Wu Z M, et al. A unified method for finding impossible differentials of block cipher structures. Inform Sci, 2014, 263: 211–220
18 Wu S B, Wang M S. Automatic search of truncated impossible differentials for word-oriented block ciphers. In: Progress in Cryptology — INDOCRYPT. Berlin: Springer, 2012. 283–302
19 Bogdanov A, Rijmen V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Design Code Cryptogr, 2014, 70: 369–383
20 Knudsen L R, Wagner D. Integral cryptanalysis. In: Revised Papers From the 9th International Workshop on Fast Software Encryption. Berlin: Springer, 2002. 112–127
21 Sun B, Li R L, Qu L J, et al. SQUARE attack on block ciphers with low algebraic degree. Sci China Inf Sci, 2010, 53: 1988–1995