Linear and Di erential Cryptanalysis of Reduced SMS4 Block Cipher

Taehyun Kim[1], Jongsung Kim[1], Seokhie Hong[1], Jaechul Sung[2]

[1] Center for Information Security Technologies (CIST),
Korea University,
{kimth714 joshep hsh}@cist.korea.ac.kr
[2] Department of Mathematics, University of Seoul, Seoul, Korea
jcsung@uos.ac.kr

Abstract SMS4 is a 128-bit block cipher with a 128-bit user key and 32 rounds, which is used in WAPI, the Chinese WLAN national standard. In this paper, we present a linear attack and a di erential attack on a 22-round reduced SMS4; our 22-round linear attack has a data complexity of 2^{117} known plaintexts, a memory complexity of $2^{1\ 9}$ bytes and a time complexity of $2^{1\ 9.86}$ 22-round SMS4 encryptions and $2^{12\ .39}$ arithmetic operations, while our 22-round di erential attack requires 2^{118} chosen plaintexts, 2^{123} memory bytes and $2^{125.71}$ 22-round SMS4 encryptions. Both of our attacks are better than any previously known cryptanalytic results on SMS4 in terms of the number of attacked rounds. Furthermore, we present a boomerang and a rectangle attacks on a 18-round reduced SMS4. These results are better than previously known rectangle attacks on reduced SMS4. The methods presented to attack SMS4 can be applied to other unbalanced Feistel ciphers with incomplete di usion.

Keywords : Block Cipher, SMS4, Linear Attack, Di erential Attack, Boomerang Attack, Rectangle Attck

1 Introduction

The Chinese national standard for Wireless Local Area Networks (WLANs), WLAN Authentication and Privacy Infrastructure (WAPI) standard is an alternative to the security mechanisms for wireless networks that are specified in IEEE 802.11i [16]. It has been submitted to the International Standards Organization ISO by Chinese Standards Association SAC. Both WAPI and IEEE 802.11i have been proposed as security amendments to the ISO/IEC 8802-11 WLAN standard. The two schemes use two di erent block ciphers for encryption of data; the WAPI uses the SMS4 block cipher [15] while the IEEE 802.11i uses the AES block cipher [14]. In contrast with AES, SMS4 did not guarantee a security by logical and formula analysis since an exact algorithm of SMS4 was not made public at the first time. In March 2006, IEEE 802.11i was approved as the ISO/IEC 8802-11 WLAN standard, while WAPI was rejected partially because

Table 1 Summary of cryptanalytic results on SMS4

Attack Type	Rounds	Complexity		
		Data	Memory	Time
Di erential [18]	21	2^{118} CP	2^{123}	$2^{126.6}$ Enc.
Rectangle [18]	16	2^{125} CP	2^{125}	2^{116} Enc.
Impossible di erential [11]	16	$2^{1\ 5}$ CP	$2^{1\ 9}$	$2^{1\ 7}$ Enc.
Rectangle [11]	14	$2^{121.82}$ CP	$2^{125.82}$	$2^{116.66}$ Enc.
Integral [10]	13	2^{16} CP	2^{2}	2^{114} Enc.
Linear (this paper)	22	2^{117} KP	$2^{1\ 9}$	$2^{1\ 9.86}$ Enc. $+2^{12\ .39}$ A.O.
Di erential (this paper)	22	2^{118} CP	2^{123}	$2^{125.71}$ Enc.
Boomerang (this paper)	18	2^{12} ACPS	2^{123}	$2^{116.83}$ Enc.
Rectangle (this paper)	18	2^{124} CP	2^{128}	$2^{112.83}$ Enc.

KP - Known plaintexts, CP - Chosen plaintexts
ACPS - Adaptive Chosen plaintexts and ciphertexts
Memory is measured in Bytes
Enc - Encryption units, A.O. - Arithmetic operation

of uncertainties regarding the security of the undisclosed SMS4 cipher. However, because WAPI is still officially mandated for Chinese national standard, WAPI continues to be used in the Chinese WLAN industry and many international corporations, such as SONY, which support WAPI in relevant products.

The SMS4 cipher [15], which was released in January 2006, is a 128-bit block cipher with a 128-bit user key and 32 rounds. So far, there have been several attacks on reduced SMS4; a 21-round di erential attack, 16-round impossible differential and rectangle attacks, and a 13-round integral attack. The best known cryptanalytic result on SMS4 prior to this work is a di erential attack on a 21-round reduced SMS4 using a 18-round di erential characteristic [18]. In this paper, we present a linear and a di erential attacks on a 22-round reduced SMS4 whose cryptanalytic results are better than the previously best known attack. In our 22-round linear and di erential attacks, we exploit a new 18-round linear approximation and a previously known 18-round di erential (used in the previous 21-round di erential attack). Furthermore, we present a boomerang [17] and a rectangle attacks [4] on a 18-round reduced SMS4 which are better than the best known rectangle attack. In order to conduct these attacks, we first devise new 15-round boomerang and rectangle distinguishers and then extend them to 16-round distinguishers using special properties of the unbalanced Feistel structure of SMS4. All our distinguishers used are mainly due to a slow di usion e ect of SMS4. The complexities of our new attacks along with previously known attacks are summarized in Table 1.

The outline of this paper is as follows: in Sect. 2, we introduce the notation used throughout this paper and describe the SMS4 algorithm as well as the methods of linear, di erential, boomerang and rectangle attacks. In Sects. 3-5,

we present our linear, di erential attacks and boomerang, rectangle attacks on reduced SMS4, and finally we conclude the paper in Sect. 6.

2 Preliminaries

2.1 Notation

We use the following notation throughout this paper, where the right most bit is referred to as the 0-th bit, i.e., the least significant bit.

- $\oplus$: bitwise logical exclusive OR (XOR).
- $\lll$: left cyclic shift operation.
- ? : arbitrary 32-bit word.
- $\|$: Concatenation.
- $Sbox(\cdot) : 8 \times 8$ bijective S-box used in SMS4.
- $X \cdot Y$: bitwise inner product between two 32-bit word vectors X and Y.

2.2 A description of the SMS4 block cipher

SMS4 is a 32-round unbalanced Feistel network whose block and key sizes are both 128 bits. The plaintext is represented as four 32-bit words $P = (P_0, P_1, P_2, P_3)$ and X^i denotes the output of the i-th round, where $i = 1, 2, ..., 32$. The encryption procedure of SMS4 is then as follows:

1. Input the plaintext $X^0 = P = (P_0, P_1, P_2, P_3)$,
2. For i $(= 1, 2, ..., 32)$
   - $P_{i\ 3} = P_{i\ 1} \oplus F(P_i \oplus P_{i\ 1} \oplus P_{i\ 2} \oplus RK_i) = P_{i\ 1} \oplus D(S(P_i \oplus P_{i\ 1} \oplus P_{i\ 2} \oplus RK_i))$,
   - $X^i = (P_i, P_{i\ 1}, P_{i\ 2}, P_{i\ 3})$,
3. Output the ciphertext $X^{32} = (P_{32}, P_{33}, P_{34}, P_{35})$,

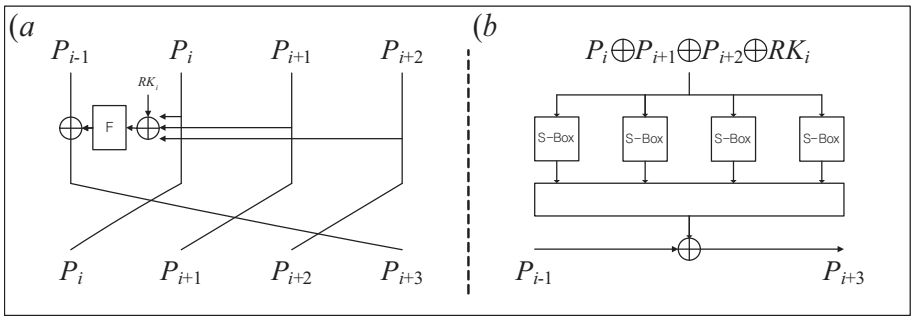

Fig 1 (a) i-th Round of SMS4, (b) F Function

Table 2 S-box table of SMS4 (e.g., $Sbox(0x01) = 0x90$)

	$0x0$	$0x1$	$0x2$	$0x3$	$0x4$	$0x5$	$0x6$	$0x7$	$0x8$	$0x9$	$0xa$	$0xb$	$0xc$	$0xd$	$0xe$	$0xf$
$0x0$	$d6$	90	$e9$	fe	cc	$e1$	$3d$	$b7$	16	$b6$	14	$c2$	28	fb	$2c$	05
$0x1$	$2b$	67	$9a$	76	$2a$	be	04	$c3$	aa	44	13	26	49	86	06	99
$0x2$	$9c$	42	50	$f4$	91	ef	98	$7a$	33	54	$0b$	43	ed	cf	ac	62
$0x3$	$e4$	$b3$	$1c$	$a9$	$c9$	08	$e8$	95	80	df	94	fa	75	$8f$	$3f$	$a6$
$0x4$	47	07	$a7$	fc	$f3$	73	17	ba	83	59	$3c$	19	$e6$	85	$4f$	$a8$
$0x5$	68	$6b$	81	$b2$	71	64	da	$8b$	$f8$	eb	$0f$	$4b$	70	56	$9d$	35
$0x6$	$1e$	24	$0e$	$5e$	63	58	$d1$	$a2$	25	22	$7c$	$3b$	01	21	78	87
$0x7$	$d4$	00	46	57	$9f$	$d3$	27	52	$4c$	36	02	$e7$	$a0$	$c4$	$c8$	$9e$
$0x8$	ea	bf	$8a$	de	40	$c7$	38	$b5$	$a3$	$f7$	$f2$	ce	$f9$	61	15	$a1$
$0x9$	$e0$	ae	$5d$	$a4$	$9b$	34	$1a$	55	ad	93	32	30	$f5$	$8c$	$b1$	$e3$
$0xa$	$1d$	$f6$	$e2$	$2e$	82	66	ca	60	$c0$	29	23	ab	$0d$	53	$4e$	$6f$
$0xb$	$d5$	db	37	45	de	fd	$8e$	$2f$	03	ff	$6a$	72	$6d$	$6c$	$5b$	51
$0xc$	$8d$	$1b$	af	92	bb	dd	bc	$7f$	11	$d9$	$5c$	41	$1f$	10	$5a$	$d8$
$0xd$	$0a$	$c1$	31	88	$a5$	cd	$7b$	bd	$2d$	74	$d0$	12	$b8$	$e5$	$b4$	$b0$
$0xe$	89	69	97	$4a$	$0c$	96	77	$7e$	65	$b9$	$f1$	09	$c5$	$6e$	$c6$	84
$0xf$	18	$f0$	$7d$	ec	$3a$	dc	$4d$	20	79	ee	$5f$	$3e$	$d7$	cb	39	48

where RK_i is the 32-bit round key for the i-th round, D is the linear di usion function defined as $D(x) = x \oplus (x \quad 2) \oplus (x \quad 10) \oplus (x \quad 18) \oplus (x \quad 24)$ and S is the nonlinear confusion function which applies a same 8×8 bijective S-box four times in parallel (see Table 2 for the S-box and Fig. 1 for a schematic description of the SMS4 round function).

The key schedule of SMS4 operates in a similar way to the encryption function. The di erence is that the di usion function $D'(x) = x \oplus (x \quad 13) \oplus (x \quad 23)$ is used instead of $D(x)$. The 128-bit user key MK is first masked with a so-called system parameter T and the resultant key is used in the key schedule function. The j-th round key RK_j is then generated as follows:

1. Input $(K_0, K_1, K_2, K_3) = (MK_0 \oplus T_0, MK_1 \oplus T_1, MK_2 \oplus T_2, MK_3 \oplus T_3,)$, where $T_0 = 0xa3b1bac6, T_1 = 0x56aa3350, T_2 = 0x677d9197, T_3 = 0xb27022dc$.
2. Output $RK_j = K_{j \ \ 3} = K_{j \ \ 1} \oplus D'(S(K_j \oplus K_{j \ \ 1} \oplus K_{j \ \ 2} \oplus CK_j))$, where the constant $CK_j = ((28 \cdot j), (28 \cdot j + 7), (28 \cdot j + 14), (28 \cdot j + 21))$ which consists of four bytes operated in Z_{256}.

2.3 The Linear Attack

Linear cryptanalysis [12], introduced by Matsui in 1993, is one of the most powerful known plaintext (or known ciphertext) attacks in symmetric-key cryptography (especially, in block ciphers and stream ciphers). It is known that this attack has similar properties to the di erential attack when analyzing some block cipher structures: [2] shows that if an r-round Feistel structure is provably secure

against the di erential attack, then it is also provably secure against the linear attack, and vice versa.

This attack investigates a correlation between the inputs and outputs for the cipher E. If for the n-bit cipher E there exists a linear approximation $\ _X \rightarrow \ _Y$ with bias ϵ such that $\epsilon > 2\ ^{\overline{2}} \cdot c^{\overline{2}}$ (or $c \cdot \epsilon\ ^2 < 2^n$), where $c > 1$, i.e.,

$$|Pr_{X,K}[\ _X \cdot X \oplus \ _Y \cdot E_K(X) = 0] \quad \frac{1}{2}| = \epsilon,$$

where $\ _X \cdot X$ and $\ _Y \cdot E_K(X)$ are both bit-wise inner products. Then the E can be distinguished from a random permutation, as the linear attack requires $\mathcal{O}(\epsilon\ ^2)$ to work by the Matsui's Algorithm 2.

2.4 The Di erential Attack

Di erential cryptanalysis [5], introduced by Biham and Shamir in 1990, is one of the most powerful chosen plaintext (or chosen ciphertext) attacks in symmetric-key cryptography (i.e., in block ciphers, stream ciphers, hash functions and MAC algorithms). After this attack was introduced, it has been applied e ectively to many known ciphers and various variants of this attack have been proposed such as the truncated di erential attack [8], the square attack [8, 7], the di erential-linear attack [9], the impossible di erential attack [3], the boomerang attack [17] and the rectangle attack [4].

This attack investigates a distribution of di erences of output pairs for the cipher E when their input pairs of E have all the same di erence. We assume that for the n-bit cipher E there exists a di erential $\Delta \rightarrow \nabla$ with probability p larger than $2\ ^n$, i.e.,

$$Pr_{X,K}[E_K(X) \oplus E_K(X \oplus \Delta) = \nabla] = p > 2\ ^n,$$

where $Pr_{X,K}[\cdot]$ is an average probability over the input X and the key K. Then the E can be distinguished from a random permutation, as the di erential holds with probability $2\ ^n$ for a random cipher.

2.5 The Boomerang and Rectangle Attacks

The boomerang attack [17] is based on two consecutive di erentials with relatively high probabilities which are independent of each other. The underlying cipher $E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ is treated as a cascade of two sub-ciphers $E = E_1 \circ E_0$, where $\{0,1\}^k$ and $\{0,1\}^n$ are the key space and the plaintext/ciphertext space, respectively. We assume that for E_0 there exists a di erential $\Delta \rightarrow \Delta^*$ with probability p and for E_1 there exists a di erential $\nabla^* \rightarrow \nabla$ with probability q. Then, these consecutive di erentials can be used e ectively to the following boomerang distinguisher:

- Ask for the encryption of a pair of plaintexts (P^1, P^2) such that $P^1 \oplus P^2 = \Delta$ and denote the corresponding ciphertexts by (C^1, C^2).

– Calculate $C^3 = C^1 \oplus \nabla$ and $C^4 = C^2 \oplus \nabla$, and ask for the decryption of the pair (C^3, C^4). Denote the corresponding plaintexts by (P^3, P^4).
– Check whether $P^3 \oplus P^4 = \Delta$.

For a random permutation the probability that the last condition is satisfied is 2^{-n}. For E, however, this probability is differently computed by the two differentials. The probability that the plaintext pair (P^1, P^2) is a right pair with respect to the first differential $\Delta \rightarrow \Delta^*$ is p, and the probability that the ciphertext pairs (C^1, C^3), (C^2, C^4) are both right pairs with respect to the second differential is q^2. If all these are right pairs, then they satisfy $E_1^{-1}(C^3) \oplus E_1^{-1}(C^4) = \Delta^* = E_0(P^3) \oplus E_0(P^4)$ as $E_1^{-1}(C^1) \oplus E_1^{-1}(C^3) = E_1^{-1}(C^2) \oplus E_1^{-1}(C^4) = \nabla^*$ and $E_1^{-1}(C^1) \oplus E_1^{-1}(C^2) = \Delta^*$ and thus, with probability p, $P^3 \oplus P^4 = \Delta$ by the first differential (note that a regular differential has a same probability for the encryption and decryption). Therefore, the total probability that the quartet of plaintexts and ciphertexts satisfies the boomerang conditions is no less than $(pq)^2$, and thus, $pq > 2^{-n/2}$ must hold for the boomerang distinguisher to work.

The rectangle attack was introduced in [4]. This is a method for eliminating the need of adaptive chosen ciphertext queries from the boomerang process. Given the same differentials the rectangle distinguisher goes as follows:

– Choose two random n-bit plaintexts P^1 and P^3 and compute two other plaintexts $P^2 = P \oplus \Delta$ and $P^4 = P^2 \oplus \Delta$.
– With a chosen plaintext attack scenario, obtain the corresponding ciphertexts C^1, C^2, C^3 and C^4.
– Check if $C^1 \oplus C^3 = C^2 \oplus C^4 = \nabla$ or $C^1 \oplus C^4 = C^2 \oplus C^3 = \nabla$

The probability that the ciphertext quartet (C^1, C^3), (C^2, C^4) satisfies the last ∇ test is computed as follows: let X^1, X^2, X^3 and X^4 denote the encrypted values of P^1, P^2, P^3 and P^4 under E_0. Then, the probability that $X^1 \oplus X^2 = X^3 \oplus X^4 = \Delta^*$ is about p^2 for E_0 by the first differential. In the above process, we randomly choose two plaintexts P^1 and P^3, so we expect $X^1 \oplus X^3 = \nabla^*$ with probability 2^{-n}. Once the two above events occur, $X^2 \oplus X^4 = (X^1 \oplus X^2) \oplus (X^3 \oplus X^4) \oplus (X^1 \oplus X^3) = \Delta^* \oplus \Delta^* \oplus \nabla^* = \nabla^*$ with probability 1. Since the probability of the second differential $\nabla^* \rightarrow \nabla$ for E_1 is q, $X^1 \oplus X^3 = X^2 \oplus X^4 = \nabla^*$ goes to $C^1 \oplus C^3 = C^2 \oplus C^4 = \nabla$ with a probability of about q^2. Similarly, we also expect $X^1 \oplus X^4 = \nabla^*$ with probability 2^{-n}, which implies $X^2 \oplus X^3 = \nabla^*$ with probability 1 (under $X^1 \oplus X^2 = X^3 \oplus X^4 = \Delta^*$ with probability p^2) and $C^1 \oplus C^4 = C^2 \oplus C^3 = \nabla$ with probability q^2. Therefore, the total probability that the last ∇ test in the above process is satisfied is no less than $2^{-n-1} \cdot p^2 \cdot q^2$.

On the other hand, for a random permutation, the ∇ test holds with probability 2^{-2n-1} and thus if the above probability is larger than 2^{-2n-1}, i.e., if $p \cdot q > 2^{-n/2}$, the rectangle distinguisher [1] can be used to distinguish E from a random permutation.

Note: The actual probabilities of the boomerang and the rectangle distinguishers are expected to be higher than the aforementioned probabilities. This

[1] More strictly, the distinguisher is called boomerang amplifier.

is due to the fact that the distinguishers hold with any intermediate di erences Δ^* and ∇^* (even any four intermediate di erences whose xor sum is zero can be contributed to the distinguishers). However, in our attacks, we only take specific Δ^* and ∇^* into account, since there is a negligible di erence in our attacks between when considering specific Δ^* and ∇^* and when considering all possible intermediate di erences.

3 Linear Attack on 22-Round SMS4

In this section, we first construct an 18-round linear approximation with bias $2^{-57.28}$ and then exploit it to devise a key recovery linear attack on 22-round SMS4.

3.1 18-round linear approximation with bias $2^{-57.28}$

All the components used in SMS4 are linear except only for the 8×8 bijective S-box. So in order to apply linear cryptanalysis to SMS4, one should first study on linear approximations of S-box. According to the linear distribution table (obtained by our computer program), the best linear approximations of the SMS4 S-box hold with bias 2^{-4} and the next with bias $2^{-4.19}$.

How can we apply these linear approximations to rounds of SMS4? Due to a structural property of the unbalanced Feistel network employed in SMS4, a same input and output mask for the F function can e ectively be used in making good linear approximations for consecutive rounds of SMS4. We have performed simulations over all possible same input and output masks for the F functions, and found that the same input and output mask $\quad = [0, 64, 6f, fe]$ o ers the best bias of $2^{-10.38}$. In this approximation, the input mask $\quad$ goes to $\quad_\gamma = [0, 6d, 13, 3]$ through the non-linear layer S with biases $2^{-4.19}$, $2^{-4.19}$ and 2^{-4} in the active S-boxes, and $\quad_\gamma$ goes to $\quad$ again through the di usion layer D. This approximation is applied to rounds 5, 6, 10, 11, 15 and 16 for designing our 18-round linear approximation for rounds 2-19. See Fig. 2 for a schematic description of our linear approximations for each of rounds 2-19. We can also mathematically express them as follows:

$$\begin{aligned}
\cdot (P_5 \oplus P_6 \oplus P_7 \oplus RK_5) &= \quad \cdot F(P_5 \oplus P_6 \oplus P_7 \oplus RK_5);\ \text{round 5},\\
\cdot (P_6 \oplus P_7 \oplus P_8 \oplus RK_6) &= \quad \cdot F(P_6 \oplus P_7 \oplus P_8 \oplus RK_6);\ \text{round 6},\\
\cdot (P_{10} \oplus P_{11} \oplus P_{12} \oplus RK_{10}) &= \quad \cdot F(P_{10} \oplus P_{11} \oplus P_{12} \oplus RK_{10});\ \text{round 10},\\
\cdot (P_{11} \oplus P_{12} \oplus P_{13} \oplus RK_{11}) &= \quad \cdot F(P_{11} \oplus P_{12} \oplus P_{13} \oplus RK_{11});\ \text{round 11},\\
\cdot (P_{15} \oplus P_{16} \oplus P_{17} \oplus RK_{15}) &= \quad \cdot F(P_{15} \oplus P_{16} \oplus P_{17} \oplus RK_{15});\ \text{round 15},\\
\cdot (P_{16} \oplus P_{17} \oplus P_{18} \oplus RK_{16}) &= \quad \cdot F(P_{16} \oplus P_{17} \oplus P_{18} \oplus RK_{16});\ \text{round 16},
\end{aligned}$$

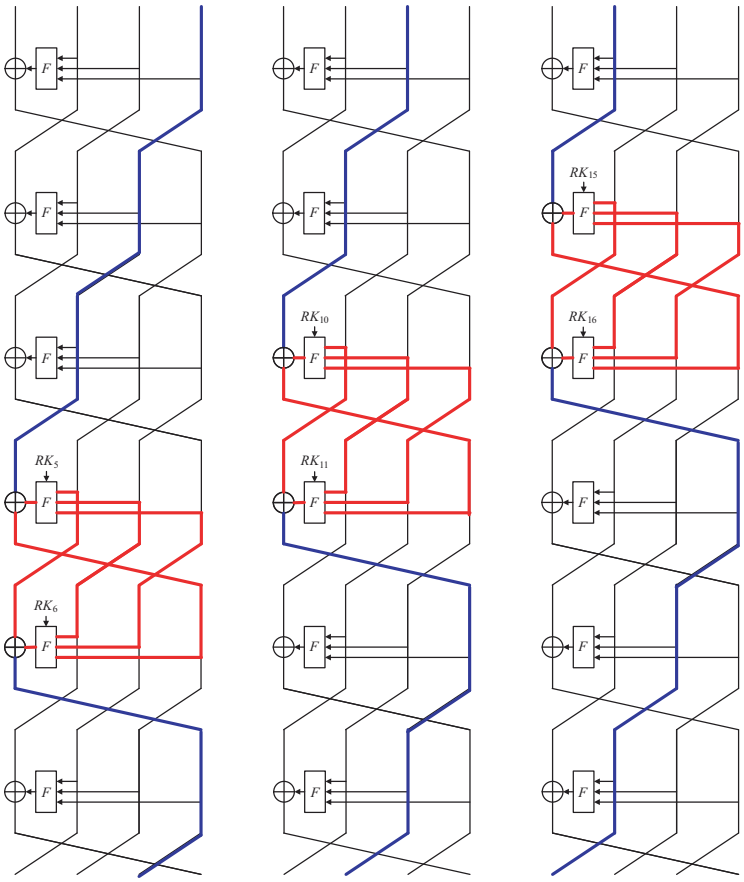

Fig 2 18-round linear approximation of SMS4

Since $F(P_i \oplus P_{i\ 1} \oplus P_{i\ 2} \oplus RK_i)$ is equal to $P_{i\ 1} \oplus P_{i\ 3}$, these approximations are summarized as

$$\begin{aligned}
\cdot P_5 \oplus \quad \cdot P_6 \oplus \quad \cdot P_7 \oplus \quad \cdot RK_5 = \quad \cdot P_4 \oplus \quad \cdot P_8, & \quad (1)\\
\cdot P_6 \oplus \quad \cdot P_7 \oplus \quad \cdot P_8 \oplus \quad \cdot RK_6 = \quad \cdot P_5 \oplus \quad \cdot P_9, & \quad (2)\\
\cdot P_{10} \oplus \quad \cdot P_{11} \oplus \quad \cdot P_{12} \oplus \quad \cdot RK_{10} = \quad \cdot P_9 \oplus \quad \cdot P_{13}, & \quad (3)\\
\cdot P_{11} \oplus \quad \cdot P_{12} \oplus \quad \cdot P_{13} \oplus \quad \cdot RK_{11} = \quad \cdot P_{10} \oplus \quad \cdot P_{14}, & \quad (4)\\
\cdot P_{15} \oplus \quad \cdot P_{16} \oplus \quad \cdot P_{17} \oplus \quad \cdot RK_{15} = \quad \cdot P_{14} \oplus \quad \cdot P_{18}, & \quad (5)\\
\cdot P_{16} \oplus \quad \cdot P_{17} \oplus \quad \cdot P_{18} \oplus \quad \cdot RK_{16} = \quad \cdot P_{15} \oplus \quad \cdot P_{19}. & \quad (6)
\end{aligned}$$

Thus, we sum over Eqs. (1), (2),...,(6) to obtain the following 18-round linear approximation;

$$\begin{aligned}
\cdot P_4 \oplus \quad \cdot P_{19} = \quad \cdot RK_5 \oplus \quad \cdot RK_6 \\
\oplus \quad \cdot RK_{10} \oplus \quad \cdot RK_{11} \oplus \quad \cdot RK_{15} \oplus \quad \cdot RK_{16}. \quad (7)
\end{aligned}$$

Note that each of Eqs. (1)-(6) has a bias of $2^{-10.38}$, and P_4 and P_{19} are output words of rounds 1 and 19, respectively (see Fig. 2). This linear approximation has a bias $2^{-57.28}(= 2^5 \cdot (2^{-10.38})^6)$ which is computed by the Pilling-up lemma [12]. The success rate of linear cryptanalysis depends significantly on the amount of the plaintexts by the Matsui's algorithm [12]. To give a high success rate (≈ 0.96), we prepare $2^{117}(\approx 2^3 \cdot (2^{57.28})^2)$ plaintexts and get their 22-round SMS4 ciphertexts $C = (C_0, C_1, C_2, C_3)$ with a known plaintext attack scenario.

3.2 Attack procedure

We conduct the Matsui's Algorithm 2 [12] to SMS4 and apply the techniques introduced in [6, 13]. The general description of the Matsui's Algorithm 2 is that an $(r \quad r')$-round linear approximation is applied to an r-round linear attack after a partial decryption of the last r' rounds is performed by guessing the key bits involved in output mask of the $(r \quad r')$-round linear approximation, which results in the recovery of all the guessed key bits. Our key recovery linear attack is applied for rounds 1-22; for rounds 2-19 our linear approximation is applied, and for the first round and the last 3 rounds the partial key guessing phase is applied which recovers a partial key of rounds 1, 20, 21 and 22 (4R-Attack), and then the exhaustive search phase for the remaining key bits is performed to recover the master key.

Matsui also proposed in [13] an improvement of the Algorithm 2 which considerably reduces the time complexity of the attack; in this improved attack, the time complexity depends only on active S-boxes in the subkey guessing phase. This improvement is applied in our linear attack. In our attack, the number of active S-boxes is 6 for rounds 1, 20, and 8 for rounds 21, 22, therefore, we need 2^{112} subkey guesses in total to evaluate the bias of our linear approximation of SMS4; we decrypt only the ciphertext bits corresponding to the active S-boxes while the original linear attack decrypts all the collected ciphertexts.

First of all, we extend Eq. (7) to the expression of a plaintext (P_0, P_1, P_2, P_3), its 22-round ciphertext $C = (C_0, C_1, C_2, C_3)$ and a subkey of rounds 1, 20, 21 and 22 $(RK_1, RK_{20}, RK_{21}, RK_{22})$; the extended expression of Eq. (7) is as follows:

$$\begin{aligned} &\cdot P_0 \oplus \quad \cdot C_1 \oplus \quad \cdot F(P_1 \oplus P_2 \oplus P_3 \oplus RK_1) \\ \oplus \quad &\cdot F(C_0 \oplus C_2 \oplus C_3 \oplus RK_{20} \oplus F(C_0 \oplus C_1 \oplus C_2 \oplus RK_{22}) \\ \oplus F(C_0 \oplus C_1 \oplus C_3 \oplus RK_{21} \oplus F(C_0 \oplus C_1 \oplus C_2 \oplus RK_{22}))) &= K(RK), \end{aligned} \tag{8}$$

where $K(RK)$ is the right side of Eq. (7). We represent Eq. (8) as the following form of equation:

$$g(P, C) \oplus f(RK, C) = K(RK), \tag{9}$$

where g is a function which evaluates a parity of the expression composed of a plaintext and its 22-round SMS4 ciphertext (the first and second terms of Eq. (8)) and f is a function composed of F functions (the rest of the left side of Eq. (8)). The value of f depends on 112 bits of the ciphertext and the round subkey, respectively, because 48 bits from $(P_1 \oplus P_2 \oplus P_3)$ and $(C_0 \oplus C_2 \oplus C_3)$ are involved due to 6 active S-boxes for rounds 1 and 20 (recall goes to $_\gamma = [0, 6d, 13, 3]$ through the inverse of the di usion layer D^{-1}) while 64 bits from $(C_0 \oplus C_1 \oplus C_2)$ and $(C_0 \oplus C_1 \oplus C_3)$ are involved due to 8 active S-boxes for rounds 21 and 22. Precisely, the parity of f is determined by the following two 112-bit vectors; $\gamma = 112$ bits of $(RK_1, RK_{20}, RK_{21}, RK_{22})$, $\delta = 112$ bits of $(P_1 \oplus P_2 \oplus P_3, C_0 \oplus C_2 \oplus C_3, C_0 \oplus C_1 \oplus C_3, C_0 \oplus C_1 \oplus C_2)$. Let $Z = Z_3 \| Z_2 \| Z_1 \| Z_0$ be 112 bits representing the bits of $\gamma \oplus \delta$ where $Z_0 = RK_{22} \oplus C_0 \oplus C_1 \oplus C_2$, $Z_1 = RK_{21} \oplus C_0 \oplus C_1 \oplus C_3$, and $Z_2 = 24$ bits of $RK_{20} \oplus C_0 \oplus C_2 \oplus C_3$, $Z_3 =$ 24 bits of $RK_1 \oplus P_1 \oplus P_2 \oplus P_3$. Consequently, $f(RK, C)$ is represented as the following equation.

$$f(RK, C) = \quad \cdot F(Z_3) \oplus \quad \cdot F(Z_2 \oplus F(Z_0) \oplus F(Z_1 \oplus F(Z_0))) \tag{10}$$

We then evaluate the bias of our approximation Eq. (9) for each key candidate using Eq. (10) and 2^{117} plaintext/ciphertext pairs. The 4R-Attack of the SMS4 is as follows:

1. Initialize a vector $\mathbf{X}$ composed of 2^{112} elements corresponding to 112 plaintext/ciphertext bits of δ used in f.
2. For each value of γ (related to subkeys) and δ (related to texts), compute the parity of the $f(\gamma, \delta)$ (parity is 1 if $f(\gamma, \delta)$ is 0, and -1 otherwise). Keep this value in a $2^{112} \times 2^{112}$ matrix $\mathbf{M}$, i.e., $\mathbf{M}[\gamma][\delta] = f(\gamma, \delta)$ (γ is for the row and δ for the column).
3. For each plaintext/ciphertext pairs, compute the parity of g. If the parity of g is 1, increase the involved counter in $\mathbf{X}$ by 1, otherwise, decrease the counter in $\mathbf{X}$ by 1 (recall that entries of $\mathbf{X}$ correspond to 112 of δ used in f).
4. Compute the bias ϵ for each key candidate (for each value of γ) by the matrix-vector product $\mathbf{M} \cdot \mathbf{X}$ (ϵ for each key candidate is proportional to the corresponding entry of $\mathbf{M} \cdot \mathbf{X}$).
5. Let ϵ_{max} be the maximal value and ϵ_{min} be the minimal value of all ϵ biases.

- If $|\epsilon_{max}| > |\epsilon_{min}|$, then adopt the key candidate corresponding to ϵ_{max} and guess $K(RK) = 0$.
- If $|\epsilon_{max}| < |\epsilon_{min}|$, then adopt the key candidate corresponding to ϵ_{min} and guess $K(RK) = 1$.

6. Once the 113-bit subkey of RK_1, RK_{20}, RK_{21}, RK_{22} and $K(RK)$ is extracted, do an exhaustive search over all possible values for the remaining 15 subkey bits for the correct master key.

In order to keep vector $\mathbf{X}$ composed of 2^{112} elements, 2^{112}-bit memory is required, equivalently 2^{108}-byte memory. In step 2, due to a *circulant structure* of the matrix $\mathbf{M}$ [6], one can the $\mathbf{M}$ much efficiently than the straightforward computation requiring $2^{112} \times 2^{112}$ operations; for each value of Z, we compute the parity of the $f(\gamma, \delta)$ and keep this value to compute the values in the relevant positions of $\mathbf{M}$. In this phase, $2^{109.8}(\approx 2^{112} \cdot 5 \cdot \frac{1}{22})$ 22-round SMS4 encryptions are required, for f calls of five F functions, and 2^{112}-bit memory is required, equivalently 2^{108}-byte memory (note that one does not need to keep every of $\mathbf{M}$, instead, he keeps 2^{112} bits according to Z and accesses the relavant values in the computation of $\mathbf{M} \cdot \mathbf{X}$). During step 3, simple operations like bit extractions and incrementations are performed, which require approximately 2^{117} arithmetic operations. In step 4, the time complexity for the evaluation of the experimental biases is $2^{224}(= 2^{112} \cdot 2^{112})$ operations as it implies a matrix-vector product with size 2^{112}. However, the fact that the matrix $\mathbf{M}$ has a *circulant structure* allows us to significantly reduce the number of operations required to evaluate the vector of the bias ϵ. B. Collard et al. first presented in [6] this method by using Fast Fourier Transform; it is possible that the matrix $\mathbf{M}$ is diagonalizable by Discrete Fourier Transform matrix, which implies that the bias can be computed using three matrix-vector product involving the Discrete Fourier Transform matrix. The multidimensional Fast Fourier Transform allows us to quickly compute the matrix-vector product. Consequently, we can perform step 4 with a complexity of $2^{120.39}(\approx 3 \cdot 112 \cdot 2^{112})$ arithmetic operations. In step 6, the exhaustive search has a time complexity of $2^{15}(= 2^{128\ \ 113})$ encryptions by the key scheduling structural property. Thus, the total time complexity is about $2^{109.8}$ 22-round SMS4 encryptions and $2^{120.39}$ arithmetic operations. To summarize, this attack requires 2^{117} known plaintexts, 2^{109} memory bytes and $2^{109.8}$ encryptions and $2^{120.39}$ arithmetic operations.

4 Di erential Attack on 22-Round SMS4

In this section, we present a 18-round di erential characteristic of SMS4 presented in [18] and show that it can be used to devise a key recovery di erential attack on 22-round SMS4.

4.1 18-round di erential characteristic with probability 2^{-26} [18]

Similarly to the linear attack, the di erential attack of SMS4 starts by studying on the nonlinear layer S, precisely, on the XOR di erence distribution of the 8×8

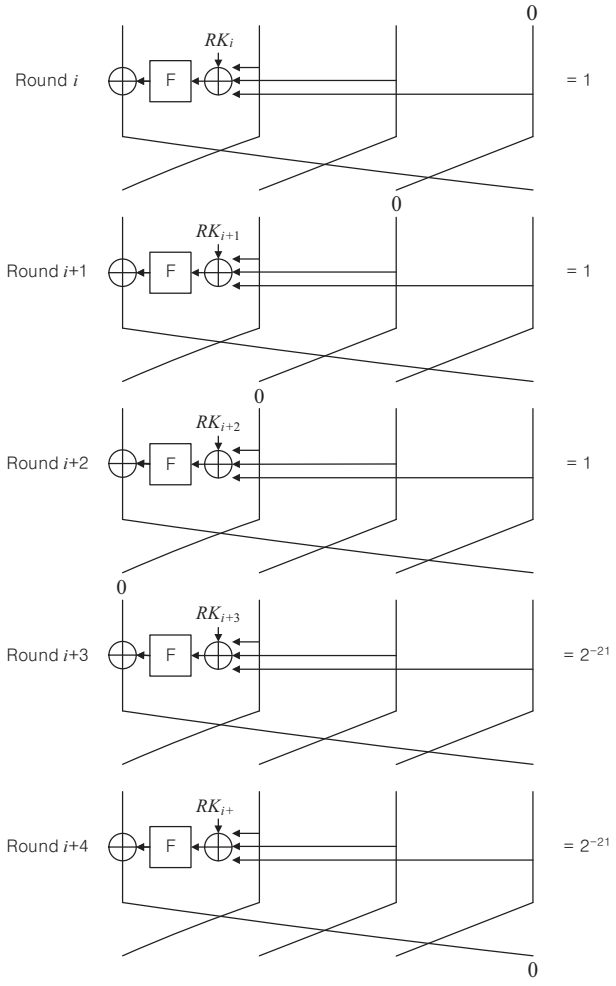

Fig 3 5-round iterative di erential characteristic of SMS4 [18]

S-box. For each input di erence value, there are 127 output di erence values of the S-box; one input/output di erence pair holds a probability 2^{-6} and the others have a probability 2^{-7}. This fact is easily proved by computer program [11]. As in our linear approximation, a same input and output di erence for the F function can e ectively be used to construct good di erential characteristics. Zhang found 7905 ($\approx 2^{13}$) possible values of α which satisfy that the di erence α goes to the same di erence α through F with probability 2^{-21} [18]. The first bytes of all the 2^{13} possible α are 0 and the rest bytes are all nonzeroes. Each nonzero byte of α holds a probability 2^{-7} through the S-box. This property allows to make a 5-round iterative di erential characteristic with probability 2^{-42} (see Fig. 3).

In [18], Zhang constructed an 18-round di erential characteristic with probability 2^{-126} ($= (2^{-42})^3$) by iterating this 5-round di erential three and half times. The 18-round di erential characteristic is described in Table 3.

Table 3 18-round Di erential characteristic and the last 4-round di erential after the characteristic

Round	Input	Cumulative Prob.
0	$(\alpha, \alpha, \alpha, 0)$	1
5	$(\alpha, \alpha, \alpha, 0)$	2^{-42}
10	$(\alpha, \alpha, \alpha, 0)$	2^{-84}
15	$(\alpha, \alpha, \alpha, 0)$	2^{-126}
16	$(\alpha, \alpha, 0, \alpha)$	2^{-126}
17	$(\alpha, 0, \alpha, \alpha)$	2^{-126}
18	$(0, \alpha, \alpha, \alpha)$	2^{-126}
19	$(\alpha, \alpha, \alpha, \Lambda)$	2^{-126}
20	$(\alpha, \alpha, \Lambda, ?)$	2^{-126}
21	$(\alpha, \Lambda, ?, ?)$	2^{-126}
22	$(\Lambda, ?, ?, ?)$	2^{-126}

4.2 Attack procedure

We extend the Zhang's 21-round di erential attack [18] to a key recovery differential attack on 22-round SMS4. The main idea behind the extension of the attack is on the early abort techniques; we guess smaller portions of subkeys and discard all the disqualified texts earlier than usual. We apply the 18-round di erential characteristic to rounds 1-18, retrieve subkeys of rounds 19, 20, 21 and 22, and then the master key. In the later analysis, Di denotes the set $\{(0, \alpha, \alpha, \alpha)\}$, where α are the aforementioned 2^{13} possible values, and $*$ denotes an unknown word. Our key recovery di erential attack is applied to 22-round SMS4 as follows:

1. Select 2^{46} structures of 2^{72} plaintexts each, where in each structure the 56 bits of bytes 0, 4, 8, 12, 13, 14, 15 are fixed, and all the other 72 bits take all the possible values. Then each structure generates about $(2^{72})^2/2 = 2^{143}$ plaintext pairs with di erence $((0,*,*,*),(0,*,*,*),(0,*,*,*),(0,0,0,0))$. Check if the di erence of each plaintext pair belongs to set Di . If this is not the case, discard the pair. After this test, about 2^{130} $(= 2^{46} \cdot 2^{143} \cdot (2^{13}/2^{72}))$ plaintext pairs are expected to remain.
2. For each remaining pair (P^i, P^j), compute the plaintex di erence and denote it as $((0,u,v,w),(0,u,v,w),(0,u,v,w),(0,0,0,0))$. Let Λ denote the set of all the $(2^7)^3$ $(\approx 127^3)$ possible 32-bit di erences $\{F(X) \oplus F(X \oplus (0,u,v,w))|X$: any 32-bit values$\}$. Compute the di erence of each corresponding ciphertext pair (C^i, C^j), and check if the first word of the ciphertext di erence belongs to set Λ (see Table 3). After this test there remains 2^{119} $(= 2^{130} \cdot (2^{21}/2^{32}))$.
3. Guess the least significant 1-byte subkey $RK_{22,0}$, and compute the output di erence of each remaining ciphertext pair after the first S-box in the F function with the guessed $RK_{22,0}$;

$$\gamma = Sbox([C_0^i \oplus C_1^i \oplus C_2^i]_{[0]} \oplus RK_{22,0}) \oplus Sbox([C_0^j \oplus C_1^j \oplus C_2^j]_{[0]} \oplus RK_{22,0}),$$
$$\delta = [D \ ^1(C_3^i \oplus C_3^j)]_{[0]},$$

   where $[X]_j$ is the j-th least significant byte of a 32-bit word X. When the guessed key $(RK_{20,0})$ is right, the value of γ is equal to δ for right pairs. If the two values are di erent, discard the ciphertext pairs used in the computation. Otherwise, the probability is 2^{-8} randomly. Hence, the number of the remaining ciphertext pairs after this step is about 2^{111} $(= 2^{119} \cdot 2^{-8})$.
4. For each of the remaining byte subkeys in rounds 22, 21 and 20, compute γ and δ similarly to step 3. Discard all the ciphertext pairs such that $\gamma \neq \delta$. Up to this step, the number of the remaining ciphertext pairs is about 2^{23} $(= 2^{111} \cdot (2^{-8})^{11})$.
5. Guess an 1-byte subkey $RK_{19,0}$, compute γ and δ with the guessed subkey, and then again discard ciphertext pairs in the same manner. We have already used a filtering probability of approximately $\frac{1}{2}$, which implies that ciphertext pairs are filtered with a probability of about $2^{-7}(\approx \frac{1}{127})$. For each $RK_{19,1}$ and $RK_{19,2}$, repeat this step. Thus the expectation of the remaining ciphertext pairs for a wrongly guessed key is about 2^2 $(= 2^{23} \cdot (2^{-7})^3)$. On the other hand, if the right key is guessed, the expectation of the ciphertext pairs after this step is 16 $(= 2^{130} \cdot 2^{-126})$. Keep the $RK_{19,0}$, $RK_{19,1}$, $RK_{19,2}$, RK_{20}, RK_{21}, RK_{22} as the candidates of the right subkey, if the number of the remaining ciphertexts is larger than or equal to 15.
6. If the subkey $RK_{19,0}$, $RK_{19,1}$, $RK_{19,2}$, RK_{20}, RK_{21}, RK_{22} is survived, do an exhaustive search over all possible values for the remaining 8 subkey bits for the correct master key.

The data complexity of this attack is about 2^{118} chosen plaintexts and the memory complexity is $2^{123}(= 2^{118} \cdot 16 \cdot 2)$ byte as it stores 2^{118} plaintext/ciphertext pairs in a table.

The time complexity of this attack is analyzed as follows. In step 3, we partially encrypt 2^{119} ciphertext pairs through one S-box with 2^8 guessed keys for $RK_{22,0}$, so its time complexity is $2^{121.54}$ ($\approx 2^{119} \cdot 2^8 \cdot 2 \cdot \frac{1}{22} \cdot \frac{1}{4}$) 22-round SMS4 encryptions. In step 4, since the number of the ciphertext pairs discarded is the same as the number of the keys guessed additionally, the time complexity is the same $2^{121.54}$ encryption for each 8-bit guessing phase in step 4 which results in $12 \cdot 2^{121.54}$ encryption in total for steps 3-4. In step 5, the time complexity is $2^{122.54}$ for each 8-bit key guessing phase as it uses a filtering probability of approximately $\frac{1}{2}$ for remaining ciphertexts, and thus the time complexity up to step 5 is about $2^{125.71}$ ($\approx 12 \cdot 2^{121.54} + 3 \cdot 2^{122.54}$) 22-round SMS4 encryptions. By the Poisson distribution $X \sim Poi(\lambda = 2^2)$, $Pr_X[X > 14] \approx 2^{-15.61}$, the expectation of wrong subkeys suggested in step 5 is about $2^{104.39}$ ($= 2^{120} \cdot 2^{-15.61}$). The exhaustive search in step 6 has a time complexity of $2^{112.39}$ ($= 2^{104.39} \cdot 2^8$) encryptions by the structural property of the key schedule. Thus, the total time complexity of this attack is approximately $2^{125.71}$ 22-round SMS4 encryptions. The success rate of this attack is 0.6 due to the fact that $Pr_X[X > 14] \approx 0.6$ by the Poisson distribution $X \sim Poi(\lambda = 2^4)$ for the right key.

5 Boomerang and Rectangle Attacks on 18-Round SMS4

In this section, we introduce 16-round boomerang and rectangle distinguishers of SMS4 and show that they can be used to devise key recovery boomerang and rectangle attacks on 18-round SMS4.

5.1 15-round boomerang and rectangle distinguishers of SMS4

The boomerang and rectangle distinguishers are both based on two short differential characteristics with high probabilities. In order to keep the number of active S-boxes in our di erential characteristics as low as possible, we use the following two di erentials through the F function;

(i) $\alpha \rightarrow \beta$ $(HW_b(\alpha) = 1, HW_b(\beta) = 4)$,
(ii) $\alpha \oplus \beta \rightarrow \alpha$ $(HW_b(\alpha \oplus \beta) = 4)$,

where $HW_b(X)$ is the *Hamming Weight* of a 32-bit word X in byte. When $\alpha \rightarrow \beta$ through F is applied, we have one active S-box, while we have four active S-boxes when $\alpha \oplus \beta \rightarrow \alpha$ through F is applied (this is due to the fact that the branch number of D is 5). In order to find these characteristics whose multiplied probability is maximal over all values corresponding to α and β, we have experimented over all possible 256 di erence values of α, and found several α to produce the maximal probability (for case (i) 2^{-6}, for case (ii) 2^{-28}). In our attack we adopt $\alpha = 00\ 00\ 00\ 09_x$ and $\beta = 72\ cd\ cd\ bf_x$. Using these two characteristics of the F function we can make a first 9-round di erential characteristic with probability 2^{-46}. Its specified di erences to each of 9 rounds along with their probabilities are presented in Table 4.

Our second 6-round di erential characteristic with probability 2^{-12} can be constructed by chopping the 9-round di erential characteristic at the both ends, and it is used for E_1 (see Table 5 for details of the second characteristic). Therefore, we can combine them to construct a 15-round boomerang distinguisher with probability 2^{-116} $(= (2^{-46})^2 \cdot (2^{-12})^2)$ and a rectangle distinguisher with probability 2^{-244} $(= 2^{-128} \cdot (2^{-46})^2 \cdot (2^{-12})^2)$. As for a random permutation, the probabilities of our distinguishers are 2^{-128} $(< 2^{-116})$ and 2^{-256} $(< 2^{-244})$, respectively.

Table 4 9-round di erential characteristic of SMS4

Round	Input	Prob.	case
i	$= (0, \alpha\ \ \beta, 0, \beta)$	1	
$i+1$	$(\alpha\ \ \beta, 0, \beta, \beta)$	2^{-6}	(i)
$i+2$	$(0, \beta, \beta, \alpha\ \ \beta)$	1	
$i+3$	$(\beta, \beta, \alpha\ \ \beta, \alpha)$	2^{-28}	(ii)
$i+4$	$(\beta, \alpha\ \ \beta, \alpha, \beta)$	1	
$i+5$	$(\alpha\ \ \beta, \alpha, \beta, \beta)$	1	
$i+6$	$(\alpha, \beta, \beta, \alpha)$	2^{-6}	(i)
$i+7$	$(\beta, \beta, \alpha, \alpha\ \ \beta)$	2^{-6}	(i)
$i+8$	$(\beta, \alpha, \alpha\ \ \beta, \beta)$	1	
$i+9$	$^* = (\alpha, \alpha\ \ \beta, \beta, \beta)$		

Table 5 6-round di erential characteristic of SMS4

Round	Input	Prob.	case
j	$\nabla^* = (\beta, \beta, \alpha\ \ \beta, \alpha)$	1	
$j+1$	$(\beta, \alpha\ \ \beta, \alpha, \beta)$	1	
$j+2$	$(\alpha\ \ \beta, \alpha, \beta, \beta)$	1	
$j+3$	$(\alpha, \beta, \beta, \alpha)$	2^{-6}	(i)
$j+4$	$(\beta, \beta, \alpha, \alpha\ \ \beta)$	2^{-6}	(i)
$j+5$	$(\beta, \alpha, \alpha\ \ \beta, \beta)$	1	
$j+6$	$\nabla = (\alpha, \alpha\ \ \beta, \beta, \beta)$		

5.2 Extension to a 16-round boomerang distinguisher of SMS4

In this subsection, we extend the 15-round boomerang distinguisher to a 16-round distinguisher with a same probability 2^{-116} by taking advantage of unbalanced Feistel structure. Denote the 16 rounds of SMS4 by $E = E_1 \circ E_* \circ E_0$, where

E_0 is rounds 1–9, E_* is round 10 and E_1 is rounds 11–16. Let P^1, P^2 be the plaintexts which follow our 9-round di erential characteristic, i.e., $P^1 \oplus P^2 = \Delta$ and the output di erence after 9 rounds of P^1 and $P^2 = \Delta^*$. Denote the output values after 9 rounds of P^1 and P^2 by (x_0, x_1, x_2, x_3) and $(x_0 \oplus \alpha, x_1 \oplus \alpha \oplus \beta, x_2 \oplus \beta, x_3 \oplus \beta)$, respectively, then the output values after 10 rounds of P^1 and P^2 are $X^1 = (x_1, x_2, x_3, t)$, $X^2 = (x_1 \oplus \alpha \oplus \beta, x_2 \oplus \beta, x_3 \oplus \beta, t')$, where $t \oplus t' = F(x_1 \oplus x_2 \oplus x_3 \oplus RK_{10}) \oplus F(x_1 \oplus x_2 \oplus x_3 \oplus \alpha \oplus \beta \oplus RK_{10}) \oplus \alpha$. Assume that on the two other faces of the boomerang we have di erence ∇^* coming from below (see Fig. 4). Let X^3 and X^4 be the intermediate values after 10 rounds of the plaintexts P^3 and P^4 whose corresponding ciphertexts $C^3 = C^1 \oplus \nabla$ and $C^4 = C^2 \oplus \nabla$, where C^1 and C^2 are the ciphertexts of P^1 and P^2. Then by our assumption $X^3 = (x_1 \oplus \beta, x_2 \oplus \beta, x_3 \oplus \alpha \oplus \beta, t \oplus \alpha)$ and $X^4 = (x_1 \oplus \alpha, x_2, x_3 \oplus \alpha, t' \oplus \alpha)$. As a consequence, their intermediate values after 1 round decryption are as follows:

$$E_*^{\ 1}(X^3) = (t \oplus \alpha \oplus F(x_1 \oplus x_2 \oplus x_3 \oplus \alpha \oplus \beta \oplus RK_{10}), x_1 \oplus \beta, x_2 \oplus \beta, x_3 \oplus \alpha \oplus \beta),$$
$$E_*^{\ 1}(X^4) = (t' \oplus \alpha \oplus F(x_1 \oplus x_2 \oplus x_3 \oplus RK_{10}), x_1 \oplus \alpha, x_2, x_3 \oplus \alpha).$$

Thus $E_*^{\ 1}(X^3) \oplus E_*^{\ 1}(X^4) = \Delta^*$ which is the output di erence of the first characteristic (the first word of α di erence is due to the fact that $t \oplus t' = F(x_1 \oplus x_2 \oplus x_3 \oplus RK_{10}) \oplus F(x_1 \oplus x_2 \oplus x_3 \oplus \alpha \oplus \beta \oplus RK_{10}) \oplus \alpha$). This 16-round boomerang distinguisher has a same probability 2^{-116} $(= (2^{-46})^2 \cdot (2^{-12})^2)$ as the 15-round boomerang distinguisher. Latter, it is used to mount a key recovery attack on 18-round SMS4.

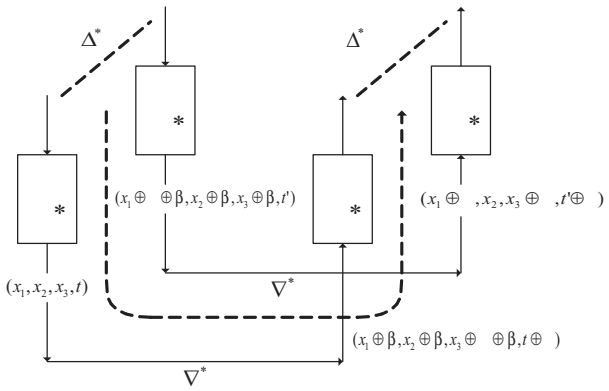

Fig 4 The free pass of the boomerang through E_*

5.3 Extension to a 16-round rectangle distinguisher of SMS4

Similarly to the process of the extension to the 16-round boomerang distinguisher, we can interleave for free a 1-round di erential into our 15-round rectangle distinguisher. Given the same 16-round SMS4 denoted by $E = E_1 \circ E_* \circ E_0$, we assume that (P^1, P^2) and (P^3, P^4) are two plaintext pairs which follow the first 9-round di erential characteristic for E_0. Denote the output values after 9 rounds of P^1, P^2, P^3 and P^4 by X^1 ,X^2, X^3 and X^4, then by our assumption,

$$\begin{aligned} X^1 &= (x_1, x_2, x_3, x_4) \\ X^2 &= (x_1 \oplus \alpha, x_2 \oplus \alpha \oplus \beta, x_3 \oplus \beta, x_4 \oplus \beta) \\ X^3 &= (x'_1, x'_2, x'_3, x'_4) \\ X^4 &= (x'_1 \oplus \alpha, x'_2 \oplus \alpha \oplus \beta, x'_3 \oplus \beta, x'_4 \oplus \beta) \end{aligned}$$

where x_i and x'_i are determined by the plaintexts and key. It follows that their output values after 1 round encryption are as follows:

$$\begin{aligned} E_*(X^1) &= (x_2, x_3, x_4, x_1 \oplus F(x_2 \oplus x_3 \oplus x_4 \oplus RK_{10})) \\ E_*(X^2) &= (x_2 \oplus \alpha \oplus \beta, x_3 \oplus \beta, x_4 \oplus \beta, x_1 \oplus \alpha \oplus F(x_2 \oplus x_3 \oplus x_4 \oplus \alpha \oplus \beta \oplus RK_{10})) \\ E_*(X^3) &= (x'_2, x'_3, x'_4, x'_1 \oplus F(x'_2 \oplus x'_3 \oplus x'_4 \oplus RK_{10})) \\ E_*(X^4) &= (x'_2 \oplus \alpha \oplus \beta, x'_3 \oplus \beta, x'_4 \oplus \beta, x'_1 \oplus \alpha \oplus F(x'_2 \oplus x'_3 \oplus x'_4 \oplus \alpha \oplus \beta \oplus RK_{10})) \end{aligned}$$

If $E_*(X^1) \oplus E_*(X^3) = \nabla^*$ with probability 2^{-128}, then the following conditions are obtained;

$$x_2 \oplus x'_2 = \beta \tag{11}$$
$$x_3 \oplus x'_3 = \beta \tag{12}$$
$$x_4 \oplus x'_4 = \alpha \oplus \beta \tag{13}$$
$$x_1 \oplus x'_1 \oplus F(x_2 \oplus x_3 \oplus x_4 \oplus RK_{10}) \oplus F(x'_2 \oplus x'_3 \oplus x'_4 \oplus RK_{10}) = \alpha \tag{14}$$

It is easy to check that summing over Eqs. (11) (12) and (13) induces the following Eq. (15)

$$x_2 \oplus x_3 \oplus x_4 = x'_2 \oplus x'_3 \oplus x'_4 \oplus \alpha \oplus \beta. \tag{15}$$

By applying Eq. (15) to Eq. (14) we have

$$\begin{aligned} &x_1 \oplus F(x_2 \oplus x_3 \oplus x_4 \oplus \alpha \oplus \beta \oplus RK_{10})) \oplus \\ &x'_1 \oplus F(x'_2 \oplus x'_3 \oplus x'_4 \oplus \alpha \oplus \beta \oplus RK_{10})) = \alpha \end{aligned} \tag{16}$$

Thus, by Eqs. (11), (12), (13) and (16), $E_*(X^2) \oplus E_*(X^4) = \nabla^*$. See Fig. 5 for an illustration of this e ect. This 16-round rectangle distinguisher has a same probability 2^{-244} $(= 2^{128} \cdot (2^{-46})^2 \cdot (2^{-12})^2)$ as the 15-round rectangle distinguisher. Later, it is used to mount a key recovery attack on 18-round SMS4.

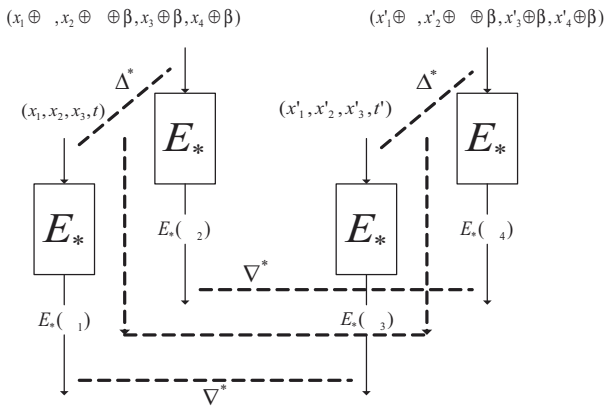

Fig 5 The free pass of the rectangle through E_*

5.4 Boomerang attack procedure

In this subsection, we introduce a boomerang attack on 18-round SMS4. We apply our 16-round boomerang distinguisher to rounds 3–18, retrieve subkeys of rounds 1 and 2, and then recover the master key. First of all, we collect plaintext structures; the plaintext pairs in each structure have a di erence of the form $(*,*,0,\alpha\oplus\beta)$. Then, we ask for encryption and decryption of each structure with a boomerang attack scenario. The key guessing phase is similar to a di erential attack; based on the 8-bit filtering property, our key recovery attack is applied to 18-round SMS4. Let Λ denote the set of all the $(2^7)^4(\approx 127^4)$ possible values of $\{F(X)\oplus F(X\oplus\alpha\oplus\beta)\oplus\beta|X$: any 32-bit values$\}$. The attack algorithm goes as follows:

1. Generate a structure $G=(S^1,S^2)$ of 2^{65} plaintexts, where S^1 and S^2 are the sets of 2^{64} plaintexts each whose forms are of $(*,*,A,B)$ and $(*,*,A,B\oplus\alpha\oplus\beta)$ for any fixed 32-bit words A and B, respectively. We prepare 2^{54} structures by changing the values of A and B (note that 2^{54} structures generate about 2^{182} $(=2^{54}\cdot(2^{64})^2)$ plaintext pairs whose di erences are of the form $(*,*,0,\alpha\oplus\beta)$, equivalently, 2^{118} $(=2^{182}\cdot 2^{\ 64})$ encrypted plaintext pairs with di erence Δ after 2 rounds).
2. Ask for the encryption of G and compute $E(G)\oplus\nabla$.
3. Ask for the decryption of $E(G)\oplus\nabla$, and denote these plaintext sets by $H=(S^3,S^4)$.
4. For all the plaintext pairs $P^3\in S^3$ and $P^4\in S^4$ in H, compute $P^3\oplus P^4$, and check if the last three words belong to $\{(\Lambda,0,\alpha\oplus\beta)\}$ (see Table 6). If not, discard corresponding the pair. After this test, there remains $2^{114}(=2^{182}\cdot 2^{\ 4}\cdot 2^{\ 32}\cdot 2^{\ 32})$ plaintext pairs in H, equivalently 2^{114} quartets in G and H, denoted (P^1,P^2,P^3,P^4), where $P^i\in S^i$.
5. Guess the least significant 1-byte subkey $RK_{1,0}$, and compute the output di erence of each remaining plaintext pair (P^3,P^4) after the first S-box in

the F function;

$$\gamma = Sbox([P_1^3 \oplus P_2^3 \oplus P_3^3]_{[0]} \oplus RK_{1,0}) \oplus Sbox([P_1^4 \oplus P_2^4 \oplus P_3^4]_{[0]} \oplus RK_{1,0}),$$
$$\delta = [D^{-1}(P_0^3 \oplus P_0^4)]_{[0]}.$$

When the guessed key ($RK_{1,0}$) is right, the value of γ is equal to δ for right quartets. If the two values are di erent, discard the plaintext quartets used in the computation. Otherwise, the probability is 2^{-8} randomly. Hence, the number of the remaining plaintext quartets after this step is about $2^{106} (= 2^{114} \cdot 2^{-8})$.

6. For the $RK_{1,0}$ guessed in step 5, compute the output di erence of each of the plaintext pairs (P^1, P^2) in G corresponding to the remaining pairs (P^3, P^4) (i.e., $P^i \in S^i$) after the first S-box in the F function;

$$\gamma = Sbox([P_1^1 \oplus P_2^1 \oplus P_3^1]_{[0]} \oplus RK_{1,0}) \oplus Sbox([P_1^2 \oplus P_2^2 \oplus P_3^2]_{[0]} \oplus RK_{1,0}),$$
$$\delta = [D^{-1}(P_0^1 \oplus P_0^2)]_{[0]}.$$

Similarly to the above step, if the two values are di erent, discard the plaintext quartets used in the computation. Hence, the number of the remaining quartets after this step is about $2^{98} (= 2^{106} \cdot 2^{-8})$.

7. For each of the remaining byte subkeys in round 1, compute γ and δ pair by pair similarly to steps 5 and 6. Discard all the plaintext quartets such that $\gamma \neq \delta$. Up to this step, the number of the remaining plaintext quartets is about $2^{50} (= 2^{98} \cdot (2^{-8})^6)$.
8. Guess an 1-byte subkey $RK_{2,0}$, compute γ and δ, and then again discard plaintext quartets in the same manner. We have already used a filtering probability of approximately $\frac{1}{2}$, which implies that plaintext quartets are filtered with probability $2^{-7} (\approx \frac{1}{127})$ at this stage. For each of $RK_{2,1}$, $RK_{2,3}$ and $RK_{2,3}$, repeat this step. Thus the expectation of the remaining plaintext quartets for a wrongly guessed key is about $2^{-6} (= 2^{50} \cdot (2^{-7})^8)$. On the other hand, if the right key is guessed, the expectation of the remaining quartets after this step is $4 (= 2^{118} \cdot 2^{-116})$ due to our 16-round boomerang distinguisher. Keep the RK_1 and RK_2 as the candidates of the right subkey, if the number of the remaining quartets is larger than or equal to 3.
9. If the subkey RK_1 and RK_2 is survived, do an exhaustive search over all possible values for the remaining 64 subkey bits for the correct master key.

Table 6 First two-round di erential before our boomerang distinguisher

Round	input di erence	Prob.
1	$(?, \Lambda, 0, \alpha \quad \beta)$	1
2	$(\Lambda, 0, \alpha \quad \beta, 0)$	1
3	$(0, \alpha \quad \beta, 0, \beta)$	

The data complexity of this attack is about 2^{120} chosen plaintexts and adaptive chosen ciphertexts as it collect 2^{54} structures of 2^{65} plaintexts each and 2^{54} structures of 2^{65} ciphertexts each, and the memory complexity is 2^{123} ($= 2^{54} \cdot 2^{65} \cdot 16$) bytes as it stores 2^{119} plaintexts of H in a table.

Step 5 encrypts 2^{114} plaintext pairs in the remaining quartets through one S-box with 2^8 guessed keys for $RK_{1,0}$, and thus its time complexity is $2^{116.83}$ ($\approx 2^{114} \cdot 2^8 \cdot 2 \cdot \frac{1}{18} \cdot \frac{1}{4}$) 18-round SMS4 encryptions. In step 6, we partially encrypt 2^{106} pairs in the remaining quartets with a guessed key for $RK_{1,0}$, so its time complexity is $2^{108.83}$ ($\approx 2^{106} \cdot 2^8 \cdot 2 \cdot \frac{1}{18} \cdot \frac{1}{4}$) 18-round SMS4 encryptions. In steps 7 and 8, the time complexity is much smaller than $2^{116.83}$ for each 8-bit key guessing phase, therefore, the time complexity up to step 8 is about $2^{116.83}$ 18-round SMS4 encryptions. By the Poisson distribution $X \sim Poi(\lambda = 2^{-6})$, $Pr_X[X > 2] \approx 2^{-20.6}$, the expectation of wrong subkeys suggested in step 9 is about $2^{43.4}$ ($= 2^{64} \cdot 2^{-20.6}$). It follows that the exhaustive search performed in step 9 has a time complexity of $2^{107.4}$ ($= 2^{43.4} \cdot 2^{64}$) encryptions. Thus, the total time complexity of this attack is approximately $2^{116.83}$ 18-round SMS4 encryptions, and the success rate of this attack is 0.7 due to the fact that $Pr_X[X > 2] \approx 0.7$ by the Poisson distribution $X \sim Poi(\lambda = 2^2)$ for the right key.

5.5 Rectangle attack procedure

In our 18-round rectangle attack, we can also conduct a 8-bit filtering process in a same manner. We apply our 16-round rectangle distinguisher to rounds 1–16, retrieve subkeys of rounds 17, 18 and then recover the master key. First of all, we choose 2^{123} plaintext pairs with a di erence Δ, which generate 2^{245} quartets. Then we compute the di erences of the ciphertext quartets (C^1, C^3) and (C^2, C^4) whose corresponding plaintext quartets satisfy $P^1 \oplus P^2 = P^3 \oplus P^4 = \Delta$, and we check if the first three words of the ciphertext di erences belong to $\{(\beta, \beta, \Lambda)\}$ (see Table 7 for the di erential propagation after our rectangle distinguisher, and see Sect. 5.4 for Λ). After this initial filtering, there remains about 2^{109} ($= 2^{245} \cdot (2^{-32} \cdot 2^{-32} \cdot 2^{28}/2^{32})^2$) ciphertext quartets. The attack procedure is similar to our boomerang attack except that we conduct a 8-bit filtering precess with ciphertext quartets instead of plaintext quartets; for each of the guessed 8-bit subkey for rounds 18 and 17, we check whether the computed di erences γ equals δ with another ciphertext pairs (C^1, C^3) in the quartets, and repeat it with ciphertext pairs (C^2, C^4) in the quartets. Since we conduct a filtering process 16 times for a 64-bit subkey RK_{18} and RK_{17}, the expectation of the remaining ciphertext quartets is about 2^{-11} ($= 2^{109} \cdot (2^{-8})^8 \cdot (2^{-7})^8$) (note that a filtering probability is 2^{-7} for each 8-bit subkey of round 17 due to the usage of the initial filtering process). We repeat this process with another 2^{109} ciphertext quartets (C^1, C^4) and (C^2, C^3) obtained by the initial filtering process of (C^1, C^4) and (C^2, C^3). If the right key is guessed, the expectation of the remaining quartets after the second iteration is about 4 ($= 2^{245} \cdot 2^{-244} + 2^{245} \cdot 2^{-244}$), otherwise 2^{-10} ($= 2^{-11} + 2^{-11}$) randomly. If the number of the remaining quartets is larger than or equal to 3, we keep the RK_{18} and RK_{17} as the candidates of the right subkey,

and output the materkey by doing an exhaustive search over all possible values for the remaining 64 subkey bits.

Table 7 Last two-round di erential after our rectangle distinguisher

Round	input di erence	Prob.
17	$(\alpha, \alpha \quad \beta, \beta, \beta)$	1
18	$(\alpha \quad \beta, \beta, \beta, \Lambda)$	1
19	$(\beta, \beta, \Lambda, ?)$	

The data complexity of this attack is about 2^{124} chosen plaintexts and the memory complexity is 2^{128} $(= 2^{123} \cdot 16 \cdot 2)$ bytes as it stores 2^{123} ciphertext pairs in a table. Similarly to our boomerang attack, the time complexity of this attack is dominated by the first 8-bit subkey guessing phase; we partially encrypt 2^{109} pairs in the remaining quartets through one S-box with 2^8 guessed keys for $RK_{18,0}$, which leads to $2^{112.83}$ $(\approx 2 \cdot 2^{109} \cdot 2^8 \cdot 2 \cdot \frac{1}{18} \cdot \frac{1}{4})$ 18-round SMS4 encryptions. Note that the expectation of wrong subkeys loaded to the last step is about $2^{31.42}$ $(= 2^{64} \cdot 2^{\ -32.58})$ by the Poisson distribution $X \sim Poi(\lambda = 2^{\ -10})$, $Pr_X[X > 2] \approx 2^{\ -32.58}$. It results in a time complexity of $2^{95.42}$ $(= 2^{31.42} \cdot 2^{64})$ encryptions for the exhaustive search phase. Therefore, the time complexity of this attack is $2^{112.83}$ 18-round SMS4 encryptions, and the success rate of this attack is 0.7 due to the fact that $Pr_X[X > 2] \approx 0.7$ by the Poisson distribution $X \sim Poi(\lambda = 2^2)$ for the right key.

6 Conclusion

In this paper, we have presented a linear and a di erential attacks on 22-round reduced SMS4, a boomerang and a rectangle attacks on 18-round reduced SMS4. To summarize, our 22-round linear attack requires 2^{117} known plaintexts, 2^{109} memory bytes, $2^{109.86}$ encryptions and $2^{120.39}$ arithmetic operations, while our 22-round di erential attack has a data complexity of 2^{118} chosen plaintexts, a memory complexity of 2^{123} bytes and a time complexity of $2^{125.71}$ encryptions. All these attacks are better than the previously best known attack on SMS4. Futhermore, we have presented best known boomerang and rectangle attacks on SMS4; our 18-round boomerang attack requires 2^{120} chosen plaintexts and adaptive chosen ciphertexts, 2^{123} memory and $2^{116.83}$ encryptions while our 18-round rectangle attack has a data complexity of 2^{124} chosen plaintexts, a memory complexity of 2^{128} bytes and a time complexity of $2^{112.83}$ encryptions. We believe that the cryptanalytic techniques presented in this paper would be useful for the future analysis of SMS4 and for other unbalanced Feistel cipher with incomplete di usion. It should be clear, however, that none of these attacks presents a realistic threat to the security of full 32-round SMS4.

References

1. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajimaand, T. Tokita, *Camellia: a 128-bit block cipher suitable for multiple platforms-design and analysis*, Proceedings of SAC 00, LNCS 2012, pp. 39–56, Springer-Verlag, 2000.
2. K. Aoki and K. Ohta, *Strict Evaluation of the Maximum Average of Di erential Probability and the Maximem Average of Linear Probability*, IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences, Vol. E-80A, No. 1, pp. 2-8, 1997.
3. E. Biham, A. Biryukov and A. Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Di erentials*, Journal of Crytology, Vol. 18, No. 4, pp. 291-311, 2005.
4. E. Biham, O. Dunkelman and N. Keller, *The Rectangle Attack - Rectangling the Serpent*, Advances in Cryptology – Proceedings of EUROCRYPT 2001, LNCS 2045, pp. 340-357, Springer-Verlag, 2001.
5. E. Biham and A. Shamir, *Di erential Cryptanalysis of DES-like Cryptosystems*, Advances in Cryptology – Proceedings of CRYPTO 1990, LNCS 537, pp. 2-21, Springer-Verlag, 1990.
6. B. Collard , F-X. Standaert, J.-J. Quisquater, *Improving the Time Complexity of Matsui's Linear Cryptanalysis*, Proceedings of ICISC'07, LNCS 4817, pp. 77–88, Springer-Verlag, 2007.
7. J. Daemen, L.R. Knudsen and V. Rijmen, *The Block Cipher Square*, Proceedings of FSE 1997, LNCS 1267, pp. 149-165, Springer-Verlag, 1997.
8. L.R. Knudsen, *Trucated and Higher Order Di erentials*, Proceedings of FSE 1994, LNCS 1008, pp. 196-211, Springer-Verlag, 1995.
9. S.K. Langford and M.E. Hellman, *Di erential-Linear Cryptanalysis*, Advances in Cryptology – Proceedings of CRYPTO 1994, LNCS 839, pp. 17-25, Springer-Verlag, 1994.
10. F. Liu, W. Ji , L. Hu, J. Ding, S. Lv, A. Pyshkin, R.-P. Weinmann, *Analysis of the SMS4 block cipher*, Proceedings of ACISP'07. LNCS 4586, pp. 158–170, Springer-Verlag, 2007.
11. J. Lu, *Attacking Reduced-Round Versions of the SMS4 Block Cipher in the Chinese WAPI Standard*, Proceedings of ICICS'07, LNCS 4861, pp. 306–318, Springer-Verlag, 2007.
12. M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology – Proceedings of EUROCRYPT 1993, LNCS 765, pp. 386-397, Springer-Verlag, 1994.
13. M. Matsui, *The First Experimental Cryptanalysis of the Data Encryption Standard*, Advances in Cryptology – CRYPTO'94, LNCS 839, pp. 1–11, Springer-Verlag, 1994.
14. National Institute of Standards and Technology, U.S.A., Advandced Encryption Standard (AES) FIPS-197, 2001.
15. Office of State Commercial Cryptography Administration, P.R. China, *The SMS4 Block Cipher (in Chinese)*. Archive available at *http://www.oscca.gov.cn/UpFile/20062101642319799O.pdf*.
16. The Institute of Electrical and Electronics Engineers (IEEE), *http://grouper.ieee.org/groups/802/11*.
17. D. Wagner, *The Boomerang Attack*, Proceedings of FSE 1999, LNCS 1636, pp. 156-170, Springer-Verlag, 1999.
18. L. Zhang, W. Zhang and W. Wu, *Cryptanalysis of Reduced-Round SMS4 Block cipher*, Proceedings of ACISP'08, 2008.