Attacking Reduced-Round Versions of the SMS4 Block Cipher in the Chinese WAPI Standard*

Jiqiang Lu

Information Security Group, Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
lvjiqiang@hotmail.com

Abstract. SMS4 is a 32-round block cipher with a 128-bit block size and a 128-bit user key. It is used in WAPI, the Chinese WLAN national standard. In this paper, we present a rectangle attack on 14-round SMS4, and an impossible differential attack on 16-round SMS4. These are better than any previously known cryptanalytic results on SMS4 in terms of the numbers of attacked rounds.

Keywords: Block cipher, SMS4, Impossible differential cryptanalysis, Rectangle attack.

1 Introduction

The Chinese national standard for Wireless Local Area Networks (WLANs), WLAN Authentication and Privacy Infrastructure (WAPI), has been the subject of extensive international debate, especially between China and USA, since over the last four years it has been a rival for IEEE 802.11i [6] for adoption as an ISO (International Organization for Standardization) international standard. WAPI and IEEE 802.11i have both been proposed as security amendments to the ISO/IEC 8802-11 WLAN standard [7]. The two schemes use two different block ciphers for encryption of data: IEEE 802.11i uses the AES [14] cipher, while WAPI uses the SMS4 [1] cipher. In March 2006, IEEE 802.11i was approved as the standard, and WAPI was rejected, partially because of uncertainties regarding the security of the undisclosed SMS4 cipher. However, because it is a Chinese national standard, WAPI continues to be used in the Chinese WLAN industry, and many international corporations, such as SONY, support WAPI in relevant products.

The SMS4 cipher was released in a Chinese version only, in January 2006 [1]; it has a 128-bit block size, a 128-bit user key, and a total of 32 rounds. To the best of our knowledge, the only previously published cryptanalytic result on the SMS4 algorithm is an integral attack [9] on 13-round SMS4, presented recently in [10]; moreover, a differential fault analysis on the SMS4 implementation was presented in [16].

In this paper, we exploit certain 12-round rectangle distinguishers with probability $2^{-237.64}$, which can be used to mount a rectangle attack on SMS4 reduced

* This work as well as the author was supported by a British Chevening / Royal Holloway Scholarship and the European Commission under contract IST-2002-507932 (ECRYPT).

S. Qing, H. Imai, and G. Wang (Eds.): ICICS 2007, LNCS 4861, pp. 306–318, 2007.

to 14 rounds. We also exploit certain 12-round impossible differentials, which enables us to mount an impossible differential attack on SMS4 reduced to 16 rounds. The attacks use the early abort technique described in [11,12,13].

The rest of this paper is organised as follows. In the next section, we describe the notation used throughout this paper and the SMS4 cipher. In Section 3, we introduce a number of properties of SMS4 and give some necessary definitions. In Sections 4 and 5, we present our cryptanalytic results. Section 6 concludes this paper.

2 Preliminaries

2.1 Notation

We use the following notation throughout this paper.

- $\oplus$: bitwise logical exclusive OR (XOR)
- $\lll i$: left rotation by i bits
- e_j : a 32-bit word with zeros in all positions but bit j, $(0 \leq j \leq 31)$
- $e_{i_1,\cdots,i_j} : e_{i_1} \oplus \cdots \oplus e_{i_j}$, $(0 \leq i_1, \cdots, i_j \leq 31)$
- ? : an arbitrary 32-bit word, where two words represented by the ? symbol may be different

The notion of difference used throughout this paper is with respect to the $\oplus$ operation. It is assumed that the least significant bit of a 32-bit word is referred as the 0-th bit and the most significant bit is referred as the 31st bit.

2.2 The SMS4 Cipher

The SMS4 [1] block cipher takes as an input a 128-bit plaintext P, represented as four 32-bit words $P = (P_0, P_1, P_2, P_3)$, and has a total of 32 rounds. Let $X^{i+1} = (X_{i+1,0}, X_{i+1,1}, X_{i+1,2}, X_{i+1,3})$ denote the four-word output of the i-th round, $(0 \leq i \leq 31)$[1]. Then, the encryption procedure of SMS4 is as follows:

1. Set $X^0 = (X_{0,0}, X_{0,1}, X_{0,2}, X_{0,3}) = (P_0, P_1, P_2, P_3)$.
2. For $i = 0$ to 31:
   - $X_{i+1,0} = X_{i,1}$,
   - $X_{i+1,1} = X_{i,2}$,
   - $X_{i+1,2} = X_{i,3}$,
   - $X_{i+1,3} = X_{i,0} \oplus \mathrm{L}(\mathrm{S}(X_{i,1} \oplus X_{i,2} \oplus X_{i,3} \oplus RK_i))$,
3. The ciphertext is $X^{32} = (X_{32,0}, X_{32,1}, X_{32,2}, X_{32,3})$,

where RK_i is the 32-bit round subkey for the i-th round, the transformation L is defined as $\mathrm{L}(x) = x \oplus (x \lll 2) \oplus (x \lll 10) \oplus (x \lll 18) \oplus (x \lll 24)$, for $x \in Z_2^{32}$, and the transformation S applies the same 8×8 bijective S-Box (see Table 1) four times in parallel to an input, and it is defined as follows.

$$input : A = (a_0, a_1, a_2, a_3) \in (Z_2^8)^4,\ output : B = (b_0, b_1, b_2, b_3) \in (Z_2^8)^4$$
$$substitution : B = \mathrm{S}(A) \Leftrightarrow b_j = \text{S-Box}(a_j),\ \text{for } j = 0, 1, 2, 3.$$

[1] Note that the first round is referred as Round 0.

Table 1. The S-Box table of SMS4

	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	d2	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

The composed transformation L ∘ S is called T in the specification document [1]. Fig. 1 depicts one encryption round of SMS4. Decryption is identical to encryption, except that the round keys are used in the reverse order.

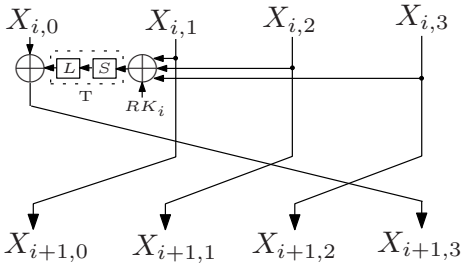

Fig. 1. The i-th encryption round of SMS4

The key schedule of SMS4 accepts a 128-bit user key MK, represented as four 32-bit words (MK_0, MK_1, MK_2, MK_3). The j-th round subkey RK_j $(0 \le j \le 31)$ is generated as follows.

- Compute $(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)$, where $FK_0 = 0xa3b1bac6, FK_1 = 0x56aa3350, FK_2 = 0x677d9197$, and $FK_3 = 0xb27022dc$.
- Compute $RK_j = K_{j+4} = K_j \oplus \mathrm{L}'(\mathrm{S}(K_{j+1} \oplus K_{j+2} \oplus K_{j+3} \oplus CK_j))$, where the transformation L′ is defined as $\mathrm{L}'(x) = x \oplus (x \lll 13) \oplus (x \lll 23)$, for $x \in Z_2^{32}$, and the constant $CK_j = (ck_{j,0}, ck_{j,1}, ck_{j,2}, ck_{j,3}) \in (Z_2^8)^4$, with $ck_{j,k} = 28j + 7k \bmod 256$ $(k = 0, 1, 2, 3)$. The composed transformation L′ ∘ S is called T′ in the specification document.

3 Properties of SMS4 and Definitions

We first introduce three properties of SMS4, which are important to our attacks.

Property 1. *For the nonlinear transformation* S, $\mathrm{S}(\Delta x) = 0$ *if, and only if,* $x = 0$ $(x \in Z_2^{32})$.

Property 2. *For the linear transformation* L, $\mathrm{L}(x) = 0$ *if, and only if,* $x = 0$ $(x \in Z_2^{32})$.

Property 3. *For the S-Box, there exist* 127 *possible output differences for any nonzero input difference, of which 1 output difference occurs with probability* 2^{-6}*, and each of the other 126 output differences occurs with probability* 2^{-7}.

Property 1 is obvious; Properties 2 and 3 can be verified by two simple computer programs.

We next give two definitions.

Definition 1. *Let* Λ *be an arbitrary but nonempty subset of any of the four sets* $\{0, 1, \cdots, 7\}$, $\{8, 9, \cdots, 15\}$, $\{16, 17, \cdots, 23\}$ *and* $\{24, 25, \cdots, 31\}$, *then we define the set* $\Omega(e_\Lambda)$ *as follows:*

$$\Omega(e_\Lambda) = \{x | x = \mathrm{L}(y), \Pr(\mathrm{S}(\Delta e_\Lambda) \rightarrow \Delta y) = 2^{-6}, x, y \in Z_2^{32}\}.$$

Note that $|\Omega(e_\Lambda)| = 1$ holds for any nonempty Λ by Property 3.

Definition 2. *Let* Λ *be an arbitrary but nonempty subset of the set* $\{0, 1, \cdots, 31\}$*; then we define the three sets* $\Theta(e_\Lambda)$, $\Upsilon(e_\Lambda, m \in \Theta(e_\Lambda))$ *and* $\Pi(e_\Lambda, m \in \Theta(e_\Lambda), n \in \Upsilon(e_\Lambda, m))$ *as follows:*

- $\Theta(e_\Lambda) = \{x | x = \mathrm{L}(y), \Pr(\mathrm{S}(\Delta e_\Lambda) \rightarrow \Delta y) > 0, x, y \in Z_2^{32}\}$.
- $\Upsilon(e_\Lambda, m \in \Theta(e_\Lambda)) = \{x | x = \mathrm{L}(y) \oplus e_\Lambda, y \in \{z | \Pr(\mathrm{S}(\Delta m) \rightarrow \Delta z) > 0, z \in Z_2^{32}\}, x, y \in Z_2^{32}\}$.
- $\Pi(e_\Lambda, m \in \Theta(e_\Lambda), n \in \Upsilon(e_\Lambda, m)) = \{x | x = \mathrm{L}(y) \oplus e_\Lambda, y \in \{z | \Pr(\mathrm{S}(\Delta(e_\Lambda \oplus m \oplus n)) \rightarrow \Delta z) > 0, z \in Z_2^{32}\}, x, y \in Z_2^{32}\}$.

4 Rectangle Attack on 14-Round SMS4

Being a variant of the boomerang attack [15] and an improvement of the amplified boomerang attack [8], the rectangle attack [4] shares the same basic idea of using two short differentials with larger probabilities instead of a long differential with a smaller probability. A rectangle attack is based on a rectangle distinguisher, which treats a block cipher $E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ as a cascade of two sub-ciphers $E = E^1 \circ E^0$.

In this section, we exploit certain 12-round rectangle distinguishers with probability $2^{-237.64}$, such that we can conduct a rectangle attack on SMS4 reduced to that operates 14 rounds.

4.1 12-Round Rectangle Distinguishers with Probability $2^{-237.64}$

Let E^0 denote Rounds 0 to 7 of SMS4, and E^1 denote Rounds 8 to 11 of SMS4. The differentials for the 12-round distinguishers are as follows.

- The following 8-round differentials $\alpha \to \beta'$ are used for E^0: $(e_{\Psi_1}, e_\Psi, e_\Psi, e_\Psi) \to (e_{\Psi_2}, e_{\Psi_3}, e_{\Psi_4}, e_{\Psi_5})$, where Ψ is an arbitrary but nonempty subset of any of the four sets $\{0, 1, \cdots, 7\}$, $\{8, 9, \cdots, 15\}$, $\{16, 17, \cdots, 23\}$ and $\{24, 25, \cdots, 31\}$, $e_{\Psi_1} \in \Omega(e_\Psi)$, $e_{\Psi_2} \in \Theta(e_\Psi)$, $e_{\Psi_3} \in \Upsilon(e_\Psi, e_{\Psi_2})$, $e_{\Psi_4} \in \Pi(e_\Psi, e_{\Psi_2}, e_{\Psi_3})$, and $e_{\Psi_5} \in \{x | x = \mathrm{L}(y) \oplus e_\Lambda, y \in \{z | Prob.(\mathrm{S}(\Delta(e_{\Psi_2} \oplus e_{\Psi_3} \oplus e_{\Psi_4})) \to \Delta z) > 0, z \in Z_2^{32}\}, x, y \in Z_2^{32}\}$.
- The following 4-round differentials $\gamma \to \delta'$ are used for E^1: $(e_\Phi, e_\Phi, e_\Phi, 0) \to (e_\Phi, e_\Phi, e_\Phi, e_{\Phi_2})$, where Φ is an arbitrary but nonempty subset of any of the four sets $\{0, 1, \cdots, 7\}$, $\{8, 9, \cdots, 15\}$, $\{16, 17, \cdots, 23\}$ and $\{24, 25, \cdots, 31\}$, $e_{\Phi_2} \in \Theta(e_\Phi)$.

See Table 2 for the details of these two groups of differentials, where the difference in a round is the input difference to this round. The same meaning is used with the differentials in the next section. Note that different Ψ and/or Φ correspond to different rectangle distinguishers. In the following, we assume Ψ and Φ are fixed.

Table 2. The two groups of differentials in the 12-round rectangle distinguisher, where † means that the probability is addressed later

Round(i)	$\Delta X_{i,0}$	$\Delta X_{i,1}$	$\Delta X_{i,2}$	$\Delta X_{i,3}$	Prob.	Round(i)	$\Delta X_{i,0}$	$\Delta X_{i,1}$	$\Delta X_{i,2}$	$\Delta X_{i,3}$	Prob.
0	e_{Ψ_1}	e_Ψ	e_Ψ	e_Ψ	2^{-6}	7	e_Ψ	e_{Ψ_2}	e_{Ψ_3}	e_{Ψ_4}	†
1	e_Ψ	e_Ψ	e_Ψ	0	1	*output*	e_{Ψ_2}	e_{Ψ_3}	e_{Ψ_4}	e_{Ψ_5}	/
2	e_Ψ	e_Ψ	0	e_Ψ	1	8	e_Φ	e_Φ	e_Φ	0	1
3	e_Ψ	0	e_Ψ	e_Ψ	1	9	e_Φ	e_Φ	0	e_Φ	1
4	0	e_Ψ	e_Ψ	e_Ψ	†	10	e_Φ	0	e_Φ	e_Φ	1
5	e_Ψ	e_Ψ	e_Ψ	e_{Ψ_2}		11	0	e_Φ	e_Φ	e_Φ	†
6	e_Ψ	e_Ψ	e_{Ψ_2}	e_{Ψ_3}		*output*	e_Φ	e_Φ	e_Φ	e_{Φ_2}	/

In the following, we need to sum the square of the probabilities of all the possible differentials $\alpha \to \beta'$. As there exist many more differential characteristics than we can count, it is infeasible to compute the exact square sum; however, we can compute a lower bound for it. By the Property 3 in Section 3, we can learn that for a fixed Ψ, there exists one e_{Ψ_2} such that the probability that $\mathrm{L}(\mathrm{S}(\Delta e_\Psi)) \to \Delta e_{\Psi_2}$ is 2^{-6}, and exist 126 e_{Ψ_2} such that the probability that $\mathrm{L}(\mathrm{S}(\Delta e_\Psi)) \to \Delta e_{\Psi_2}$ is 2^{-7}. Due to the L transformation, the four 32-bit words in any e_Ψ are all nonzero. Thus, for any e_{Ψ_2}, if we define the *Event* A: $(\mathrm{L}(\mathrm{S}(\Delta e_{\Psi_2})) \oplus e_\Psi) \to \Delta e_{\Psi_3}$, then we can learn that there exists one possible e_{Ψ_3} with probability 2^{-24}, and exist $\binom{4}{3} \cdot 126$ possible e_{Ψ_3} with probability 2^{-25}, $\binom{4}{2} \cdot 126^2$ possible e_{Ψ_3} with probability 2^{-26}, $\binom{4}{1} \cdot 126^3$ possible e_{Ψ_3} with probability 2^{-27} and 126^4 possible e_{Ψ_3} with probability 2^{-28}. Consequently, for any e_{Ψ_2} and e_{Ψ_3}, if we

define the *Event* B: $(\mathrm{L}(\mathrm{S}(\Delta(e_\Psi \oplus e_{\Psi_2} \oplus e_{\Psi_3}))) \oplus e_\Psi) \to \Delta e_{\Psi_4}$, then there exists one possible e_{Ψ_4} with probability 2^{-24}, and exist $\binom{4}{3} \cdot 126$ possible e_{Ψ_4} with probability 2^{-25}, $\binom{4}{2} \cdot 126^2$ possible e_{Ψ_4} with probability 2^{-26}, $\binom{4}{1} \cdot 126^3$ possible e_{Ψ_4} with probability 2^{-27} and 126^4 possible e_{Ψ_4} with probability 2^{-28}. Therefore, we can compute a square sum of at least $(2^{-6})^2 \cdot [(2^{-6})^2 + 126 \cdot (2^{-7})^2] \cdot [1 \cdot (2^{-24})^2 + \binom{4}{3} \cdot 126 \cdot (2^{-25})^2 + \binom{4}{2} \cdot 126^2 \cdot (2^{-26})^2 + \binom{4}{1} \cdot 126^3 \cdot (2^{-27})^2 + 126^4 \cdot (2^{-28})^2]^3 \approx 2^{-109.64}$.

For the 4-round differentials $\gamma \to \delta'$, as mentioned earlier, there are 127 possible e_{Φ_2}, 1 possibility with probability 2^{-6} and each of the other 126 possibilities with probability 2^{-7}, thus, this 12-round rectangle distinguisher has a probability of at least $2^{-109.64} \cdot [(1 \cdot 2^{-6} + 126 \cdot 2^{-7})]^2 \cdot 2^{-128} \approx 2^{-237.64}$ for the correct key, while it has a probability of $(2^{-128} \cdot 127)^2 \approx 2^{-242.02}$ for a wrong key.

The 12-round distinguisher can be used to mount a rectangle attack on 14-round SMS4. Without loss of generality, we assume the attacked 14 rounds are the first 14 rounds from Rounds 0 to 13. Given the 127 input differences $(e_\Phi, e_\Phi, e_\Phi, e_{\Phi_2})$ to Round 12, there are at most 127^5 possible output differences $\{(e_\Phi, e_\Phi, e_{\Phi_2}, e_{\Phi_3}) | e_{\Phi_3} \in \Upsilon(e_\Phi, e_{\Phi_2})\}$ just after Round 12, and at most 127^9 possible output differences $\{(e_\Phi, e_{\Phi_2}, e_{\Phi_3}, e_{\Phi_4}) |\ e_{\Phi_3} \in \Upsilon(e_\Phi, e_{\Phi_2}), e_{\Phi_4} \in \Pi(e_\Phi, e_{\Phi_2}, e_{\Phi_3})\}$ just after Round 13.

As mentioned in the Introduction, our rectangle attack, as well as the impossible differential attack in the next section, uses the early abort technique introduced in [11,12,13]; the main idea of the early abort technique is to partially determine whether or not a candidate quartet in a rectangle attack (or a candidate pair in an impossible differential attack) is valid earlier than usual, by guessing only a small fraction of subkeys required; if not, we can discard it immediately, which results in less computations in the left steps and may allow us to break more rounds by guessing the subkeys involved, depending on how many candidates are remaining.

The attack procedure is as follows.

4.2 Attack Procedure

1. Choose $2^{120.82}$ pairs of plaintexts $(P_i, \widetilde{P}_i)$ with difference $(e_{\Psi_1}, e_\Psi, e_\Psi, e_\Psi)$, $i = 1, 2, \cdots, 2^{120.82}$. In a chosen-plaintext attack scenario, obtain their corresponding ciphertext pairs; we denote them by $(C_i, \widetilde{C}_i)$, respectively. These ciphertext pairs generate about $2^{120.82 \times 2}/2 = 2^{240.64}$ candidate quartets $((C_{i_1}, \widetilde{C}_{i_1}), (C_{i_2}, \widetilde{C}_{i_2}))$, for $1 \le i_1 \le i_2 \le 2^{120.82}$. We only choose those such that both $C_{i_1} \oplus C_{i_2}$ and $\widetilde{C}_{i_1} \oplus \widetilde{C}_{i_2}$ belong to $\{(e_\Phi, e_{\Phi_2}, e_{\Phi_3}, e_{\Phi_4}) | e_{\Phi_3} \in \Upsilon(e_\Phi, e_{\Phi_2}), e_{\Phi_4} \in \Pi(e_\Phi, e_{\Phi_2}, e_{\Phi_3})\}$.
2. For all the remaining quartets $((C_{i_1}, \widetilde{C}_{i_1}), (C_{i_2}, \widetilde{C}_{i_2}))$, do as follows.
   (a) For (C_{i_1}, C_{i_2}), compute the four-byte difference of their intermediate values just before the L transformation in Round 13; we denote them by $(\Delta^{13}_{i_1,i_2,0}, \Delta^{13}_{i_1,i_2,1}, \Delta^{13}_{i_1,i_2,2}, \Delta^{13}_{i_1,i_2,3})$, respectively. For $(\widetilde{C}_{i_1}, \widetilde{C}_{i_2})$, compute the four-byte difference of their intermediate values just before the L transformation in Round 13; we denote them by $(\widetilde{\Delta}^{13}_{i_1,i_2,0}, \widetilde{\Delta}^{13}_{i_1,i_2,1}, \widetilde{\Delta}^{13}_{i_1,i_2,2}, \widetilde{\Delta}^{13}_{i_1,i_2,3})$, respectively.

(b) For $j = 0$ to 3: Guess the j-th byte $RK_{13,j}$ of the subkey RK_{13} in Round 13, and partially decrypt every remaining quartet $((C_{i_1}, C_{i_2}), (\widetilde{C}_{i_1}, \widetilde{C}_{i_2}))$ with $RK_{13,j}$ to get the j-th bytes of their intermediate values just after the S transformation in Round 13; we denote them by $((T_{i_1,j}, T_{i_2,j}), (\widetilde{T}_{i_1,j}, \widetilde{T}_{i_2,j}))$, respectively. Finally, check if $T_{i_1,j} \oplus T_{i_2,j} = \Delta^{13}_{i_1,i_2,j}$ and $\widetilde{T}_{i_1,j} \oplus \widetilde{T}_{i_2,j} = \widetilde{\Delta}^{13}_{i_1,i_2,j}$. If 6 or more quartets pass this test, execute next with them, (otherwise, repeat this iteration with another key guess).
Finally, for every remaining $((C_{i_1}, \widetilde{C}_{i_1}), (C_{i_2}, \widetilde{C}_{i_2}))$ we get their intermediate values just after Round 12; we denote them by $((T_{i_1}, \widetilde{T}_{i_1}), (T_{i_2}, \widetilde{T}_{i_2}))$, respectively.

3. For all the quartets $((T_{i_1}, \widetilde{T}_{i_1}), (T_{i_2}, \widetilde{T}_{i_2}))$, do as follows.
   (a) For (T_{i_1}, T_{i_2}), compute the four-byte difference of their intermediate values just before the L transformation in Round 12; we denote them by $(\Delta^{12}_{i_1,i_2,0}, \Delta^{12}_{i_1,i_2,1}, \Delta^{12}_{i_1,i_2,2}, \Delta^{12}_{i_1,i_2,3})$, respectively. For $(\widetilde{T}_{i_1}, \widetilde{T}_{i_2})$, compute the four-byte difference of their intermediate values just before the L transformation in Round 12; we denote them by $(\widetilde{\Delta}^{12}_{i_1,i_2,0}, \widetilde{\Delta}^{12}_{i_1,i_2,1}, \widetilde{\Delta}^{12}_{i_1,i_2,2}, \widetilde{\Delta}^{12}_{i_1,i_2,3})$, respectively.
   (b) For $j = 0$ to 3: Guess the j-th byte $RK_{12,j}$ of the subkey RK_{12} in Round 12, partially decrypt every quartet $((T_{i_1}, T_{i_2}), (\widetilde{T}_{i_1}, \widetilde{T}_{i_2}))$ with $RK_{12,j}$ to get the j-th bytes of their intermediate values just after the S transformation in Round 12; we denote them by $((Q_{i_1,j}, Q_{i_2,j}), (\widetilde{Q}_{i_1,j}, \widetilde{Q}_{i_2,j}))$, respectively. Finally, check if $Q_{i_1,j} \oplus Q_{i_2,j} = \Delta^{12}_{i_1,i_2,j}$ and $\widetilde{Q}_{i_1,j} \oplus \widetilde{Q}_{i_2,j} = \widetilde{\Delta}^{12}_{i_1,i_2,j}$. If 6 or more quartets pass this test, execute next with them, (otherwise, repeat this iteration with another key guess).
4. For every (RK_{12}, RK_{13}) passing Step 3, we can deduce that there are at most 2^{64} possible 128-bit user keys from these two 32-bit subkeys. Then, we do a trial encryption with one known pair of plaintext and ciphertext. If a 128-bit key is suggested, output it as the user key of the 14-round SMS4; otherwise, go to Step 2-(b).

To produce a difference $(e_\Phi, e_\Phi, e_\Phi, e_{\Phi_2})$ just before Round 12, the two ciphertext pairs in a right quartet must have differences belonging to the set $\{(e_\Phi, e_{\Phi_2}, e_{\Phi_3}, e_{\Phi_4}) | e_{\Phi_3} \in \Upsilon(e_\Phi, e_{\Phi_2}), e_{\Phi_4} \in \Pi(e_\Phi, e_{\Phi_2}, e_{\Phi_3})\}$, so a candidate quartet that does not meet this filtering condition is an incorrect quartet. As a result, only about $2^{240.64} \cdot (\frac{127^9}{2^{128}})^2 \approx 2^{110.46}$ candidate quartets are chosen in Step 1.

In Steps 2-(b) and 3-(b), a candidate quartet passes every test with a probability of $(\frac{1}{127})^2 \approx 2^{-13.98}$, and the number of the pairs passing every step has a binomial distribution, so it is expected that almost all the 2^{56} guesses of $(RK_{12,0}, RK_{12,1}, RK_{12,2}, RK_{13,0}, RK_{13,1}, RK_{13,2}, RK_{13,3})$ will pass the test with $j = 2$ in Step 3-(b), and for every guess about $2^{110.46} \cdot 2^{-13.98 \times 7} = 2^{12.6}$ candidate quartets are expected to remain after the test with $j = 2$ in Step 3-(b). In the test with $j = 3$ in Step 3-(b), the probability that 6 or more quartets pass the tests for a wrong guess is approximately $\sum_{i=6}^{2^{12.6}} [\binom{2^{12.6}}{i} \cdot (2^{-13.98})^i \cdot (1 - 2^{-13.98})^{2^{12.6}-i}] \approx 2^{-17.77}$, thus it is expected that about $2^{64} \cdot 2^{-17.77} = 2^{46.23}$

Table 3. The two 6-round differentials in the 12-round impossible differentials, where $x_i \in \Theta(e_\Gamma), y_i \in \Upsilon(e_\Gamma, x_i), z_i \in \Pi(e_\Gamma, x_i, y_i)$, $(i = 1, 2)$

Round$(i)\downarrow$	$\Delta X_{i,0}$	$\Delta X_{i,1}$	$\Delta X_{i,2}$	$\Delta X_{i,3}$	Round$(i)\uparrow$	$\Delta X_{i,0}$	$\Delta X_{i,1}$	$\Delta X_{i,2}$	$\Delta X_{i,3}$
0	e_Γ	e_Γ	e_Γ	0	6	z_2	y_2	x_2	e_Γ
1	e_Γ	e_Γ	0	e_Γ	7	y_2	x_2	e_Γ	e_Γ
2	e_Γ	0	e_Γ	e_Γ	8	x_2	e_Γ	e_Γ	e_Γ
3	0	e_Γ	e_Γ	e_Γ	9	e_Γ	e_Γ	e_Γ	0
4	e_Γ	e_Γ	e_Γ	x_1	10	e_Γ	e_Γ	0	e_Γ
5	e_Γ	e_Γ	x_1	y_1	11	e_Γ	0	e_Γ	e_Γ
output	e_Γ	x_1	y_1	z_1	*output*	0	e_Γ	e_Γ	e_Γ

guesses of (RK_{12}, RK_{13}) are suggested after the test with $j = 3$ in Step 3-(b). In Step 4, the expected number of wrong 128-bit keys is about $2^{-128} \cdot 2^{46.23+64} = 2^{-17.77}$, which is very low.

The attack requires $2^{121.82}$ chosen plaintexts. The required memory space is dominated by the ciphertexts, which is about $2^{121.82} \cdot 16 = 2^{125.82}$ memory bytes. The time complexity of Steps 2–4 is dominated by the partial decryptions for $j = 0$ in Step 2-(b), which is about $4 \cdot 2^8 \cdot 2^{110.46} \cdot \frac{1}{14} \approx 2^{116.66}$ 14-round SMS4 computations.

As the probability of the distinguisher is $2^{-237.64}$, it is expect there are $8 (= 2^{240.64} \cdot 2^{-237.64})$ right quartets for the correct key in Step 3-(c). The probability that 6 or more quartets pass the test in Step 3-(c) for the correct subkeys is approximately $\sum_{i=6}^{2^{240.64}} [\binom{2^{240.64}}{i} \cdot (2^{-237.64})^i \cdot (1 - 2^{-237.64})^{2^{240.64}-i}] \approx 0.8$, therefore, with a success probability of 80%, this related-key rectangle attack can break 14-round SMS4, faster than an exhaustive key search.

5 Impossible Differential Attack on 16-Round SMS4

An impossible differential [2] is a differential [5] with a zero probability; that is, it would never happen under any situation.

In this section, we exploit certain 12-round impossible differentials in SMS4. Finally, we show that impossible differential cryptanalysis can break SMS4 reduced to 16 rounds.

5.1 12-Round Impossible Differentials

The 12-round impossible differentials are $(e_\Gamma, e_\Gamma, e_\Gamma, 0) \nrightarrow (0, e_\Gamma, e_\Gamma, e_\Gamma)$, where Γ is defined as an arbitrary but nonempty subset of the set $\{0, 1, \cdots, 15\}$. These 12-round impossible differentials are built in a miss-in-the-middle manner [3]: a 6-round differential with probability 1 is concatenated with another 6-round differential with probability 1, but the intermediate differences of these two differentials contradict one another. See Table 3.

The first 6-round differential with probability 1 is $(e_\Gamma, e_\Gamma, e_\Gamma, 0) \rightarrow (e_\Gamma, ?, ?, ?)$. The input difference $(e_\Gamma, e_\Gamma, e_\Gamma, 0)$ to Round 0 propagates with probability 1

to the difference $(e_\Gamma, e_\Gamma, 0, e_\Gamma)$ after one round, which then propagates with a 1 probability to the difference $(0, e_\Gamma, e_\Gamma, e_\Gamma)$ after the following two rounds. Then, the difference $(0, e_\Gamma, e_\Gamma, e_\Gamma)$ definitely propagates to a difference belonging to the set $\{(e_\Gamma, e_\Gamma, e_\Gamma, x_1)|x_1 \in \Theta(e_\Gamma)\}$ after Round 3, which finally propagates with probability 1 to a difference belonging to $\{(e_\Gamma, x_1, y_1, z_1)|x_1 \in \Theta(e_\Gamma), y_1 \in \Upsilon(e_\Gamma, x_1), z_1 \in \Pi(e_\Gamma, x_1, y_1)\}$ after Rounds 4 and 5. On the other hand, when we roll back the output difference $(0, e_\Gamma, e_\Gamma, e_\Gamma)$ of the second 6-round differential through the three consecutive rounds from Rounds 9 to 11 in the reverse direction, we will get the difference $(e_\Gamma, e_\Gamma, e_\Gamma, 0)$ just before Round 9 with probability 1. Then, when we roll back the difference $(e_\Gamma, e_\Gamma, e_\Gamma, 0)$ through Round 8, we will definitely get a difference belonging to the set $\{(x_2, e_\Gamma, e_\Gamma, e_\Gamma)|\ x_2 \in \Theta(e_\Gamma)\}$. Finally, when we continue to go back for two more rounds, we can definitely get a difference belonging to the set $\{(z_2, y_2, x_2, e_\Gamma)|\ x_2 \in \Theta(e_\Gamma), y_2 \in \Upsilon(e_\Gamma, x_2), z_2 \in \Pi(e_\Gamma, x_2, y_2)\}$ just before Round 6. Now, a contradiction occurs, for we never get the one-round output difference $\{(y_2, x_2, e_\Gamma, e_\Gamma)|\ x_2 \in \Theta(e_\Gamma), y_2 \in \Upsilon(e_\Gamma, x_2)\}$ given an input difference belonging to $\{(e_\Gamma, x_1, y_1, z_1)|\ x_1 \in \Theta(e_\Gamma), y_1 \in \Upsilon(e_\Gamma, x_1), z_1 \in \Pi(e_\Gamma, x_1, y_1)\}$. More specifically, to get a one-round output difference belonging to $\{(y_2, x_2, e_\Gamma, e_\Gamma)|\ x_2 \in \Theta(e_\Gamma), y_2 \in \Upsilon(e_\Gamma, x_2)\}$, the input difference of the second 6-round differential should belong to the set $\{(z_2, y_2, x_2, e_\Gamma)|\ x_2 \in \Theta(e_\Gamma), y_2 \in \Upsilon(e_\Gamma, x_2), z_2 \in \Pi(e_\Gamma, x_2, y_2)\}$, however, note that the output difference of the first 6-round differential is $\{(e_\Gamma, x_1, y_1, z_1)|\ x_1 \in \Theta(e_\Gamma), y_1 \in \Upsilon(e_\Gamma, x_1), z_1 \in \Pi(e_\Gamma, x_1, y_1)\}$, so it is a necessary that the following five conditions should hold for some sextuple $(x_1, y_1, z_1, x_2, y_2, z_2)$, where $x_1, x_2 \in \Theta(e_\Gamma)$, $y_1 \in \Upsilon(e_\Gamma, x_1)$, $y_2 \in \Upsilon(e_\Gamma, x_2)$, $z_1 \in \Pi(e_\Gamma, x_1, y_1)$ and $z_2 \in \Pi(e_\Gamma, x_2, y_2)$:

$$x_2 = y_1, \tag{1}$$

$$y_2 = x_1, \tag{2}$$

$$z_1 = e_\Gamma, \tag{3}$$

$$z_2 = e_\Gamma, \tag{4}$$

$$\mathrm{L}(\mathrm{S}(x_1 \oplus y_1 \oplus e_\Gamma)) \oplus e_\Gamma = e_\Gamma. \tag{5}$$

By Properties 1 and 2 in Section 3, we can learn that Eq. (5) is equivalent to the following equation:

$$x_1 \oplus y_1 \oplus e_\Gamma = 0. \tag{6}$$

We perform a computer search over all the possibilities that may satisfy Eqs. (1)–(4) and (6), but find that there does not exist such a qualified sextuple $(x_1, y_1, z_1, x_2, y_2, z_2)$ for any nonempty subset Γ of the set $\{0, 1, \cdots, 15\}$. Thus, these 12-round impossible differentials are impossible.

Before further proceeding, we would like to give the following two remarks: i) We did not check whether there also exist similar 12-round impossible differentials if Γ is defined as an arbitrary but nonempty subset of the set $\{0, 1, \cdots, 31\}$ (excluding those described above), for this is much more time-consuming due to a sharp increase on the number of the possible differences. It is reasonably

thought that there also exist similar 12-round impossible differentials for them. ii) We did not check whether one or more of the 12-round impossible differentials can be extended to 13-round impossible differentials by appending one-round differential $(e_\Gamma, x_1, y_1, z_1) \rightarrow (x_1, y_1, z_1, ?)$ after the first 6-round differential or one-round differential $(?, z_2, y_2, x_2) \rightarrow (z_2, y_2, x_2, e_\Gamma)$ before the second 6-round differential; as there are so many possibilities (some may be identical) for any Γ that we do not have an enough powerful computer/workstation on our hands to check these possibilities with a bearable running time.

We can use a 12-round impossible differential to conduct an impossible differential attack on SMS4 reduced to 16 rounds, by taking advantage of the early abort technique introduced in [13]. We assume the attacked 16 rounds are from Rounds 0 to 15. To reduce the data and time complexities of the attack, we choose $\Gamma = \{0, 1, \cdots, 15\}$. We use the 12-round impossible differential from Rounds 2 to 13. Given the output difference $(e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, 0)$ of Round 1, there are 127^2 possible input differences to Round 1, and at most 127^6 possible input differences to Round 0; we denote them by the set Σ_1. Given the input difference $(0, e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, e_{0,1,\cdots,15})$ to Round 14, there are at most 127^2 possible output differences just after Round 14, and at most 127^6 possible output differences just after Round 15; we denote them by the set Σ_2. The attack procedure is as follows.

5.2 Attack Procedure

1. Select 2^9 structures of 2^{96} plaintexts each, where the most significant 16 bits of the rightmost two words of the plaintexts in a structure are fixed to certain values, and all the other 96 bit positions take all the possible values. Each structure generates $(2^{96}/2)^2 = 2^{190}$ plaintext pairs (P_i, P_j) with difference $(?, ?, e_{0,1,\cdots,15}, e_{0,1,\cdots,15})$; thus, the 2^9 structures propose 2^{199} plaintext pairs with difference $(?, ?, e_{0,1,\cdots,15}, e_{0,1,\cdots,15})$. In a chosen-plaintext attack scenario, obtain all the ciphertexts of P_i and P_j; we denote them by C_i and C_j, respectively. Choose only the ciphertext pairs (C_i, C_j) such that $P_i \oplus P_j \in \Sigma_1$ and $C_i \oplus C_j \in \Sigma_2$.
2. For all the remaining pairs (C_i, C_j), compute the four-byte difference of their intermediate values just before the L transformation in Round 15; we denote them by $(\Delta^{15}_{i,j,0}, \Delta^{15}_{i,j,1}, \Delta^{15}_{i,j,2}, \Delta^{15}_{i,j,3})$, respectively. Do as follows.
   (a) For $l = 0$ to 3: Guess the l-th byte $RK_{15,l}$ of the subkey RK_{15} in Round 15, partially decrypt (C_i, C_j) with $RK_{15,l}$ to get the l-th bytes of their intermediate values just after the S transformation in Round 15; we denote them by $(T_{i,l}, T_{j,l})$, respectively, and keep the pairs such that $T_{i,l} \oplus T_{j,l} = \Delta^{15}_{i,j,l}$.

   Finally, for every remaining (C_i, C_j) we can get their intermediate values just after Round 14 under the guess for RK_{15}; we denote them by (T_i, T_j), respectively.

(b) For all the remaining pairs (T_i, T_j), compute the four-byte difference of their intermediate values just before the L transformation in Round 14; we denote the first two bytes by $(\Delta^{14}_{i,j,0}, \Delta^{14}_{i,j,1})$, respectively.
(c) For $l = 0$ to 1: Guess the l-th byte $RK_{14,l}$ of the subkey RK_{14} in Round 14, partially decrypt (T_i, T_j) with $RK_{14,l}$ to get the l-th bytes of their intermediate values just after the S transformation in Round 14; we denote them by $(Q_{i,l}, Q_{j,l})$, respectively, and keep only the pairs such that $Q_{i,l} \oplus Q_{j,l} = \Delta^{14}_{i,j,l}$.

3. For all the plaintext pairs (P_i, P_j) corresponding to the remaining ciphertext pairs (C_i, C_j) after Step 2-(c), compute the four-byte difference of their intermediate values just before the L transformation in Round 0; we denote them by $(\Delta^0_{i,j,0}, \Delta^0_{i,j,1}, \Delta^0_{i,j,2}, \Delta^0_{i,j,3})$, respectively. Do as follows.
(a) For $l = 0$ to 3: Guess the l-th byte $RK_{0,l}$ of the subkey RK_0 in Round 0, partially decrypt (P_i, P_j) with $RK_{0,l}$ to get the l-th bytes of their intermediate values just after the S transformation in Round 0; we denote them by $(R_{i,l}, R_{j,l})$, respectively, and keep only the pairs such that $R_{i,l} \oplus R_{j,l} = \Delta^0_{i,j,l}$.
Finally, for every remaining (P_i, P_j) we can get their intermediate values just after Round 0 under the guess for RK_0; we denote them by (R_i, R_j), respectively.
(b) For all the remaining pairs (R_i, R_j), compute the four-byte difference of their intermediate values just before the L transformation in Round 1; we denote the first two bytes by $(\Delta^1_{i,j,0}, \Delta^1_{i,j,1})$, respectively.
(c) Guess the first byte $RK_{1,0}$ of the subkey RK_1 in Round 1, and partially decrypt (R_i, R_j) with $RK_{1,0}$ to get the first bytes of their intermediate values just after the S transformation in Round 1; we denote them by $(S_{i,0}, S_{j,0})$, respectively. Keep only the pairs such that $S_{i,0} \oplus S_{j,0} = \Delta^1_{i,j,0}$.
(d) Guess the second byte $RK_{1,1}$ of the subkey RK_1 in Round 1, partially decrypt (R_i, R_j) with $RK_{1,1}$ to get the second bytes of their intermediate values just after the S transformation in Round 1; we denote them by $(S_{i,1}, S_{j,1})$, respectively, and check if $S_{i,1} \oplus S_{j,1} = \Delta^1_{i,j,1}$. If there exists a qualified pair, then discard the guess of the 96 subkey bits, and try another; otherwise, record it, and execute Step 4.

4. For a recorded guess of the 96 subkey bits, we can deduce that there are at most 2^{96} possible 128-bit user keys from these two 32-bit subkeys. Then, we do a trial encryption with one known pair of plaintext and ciphertext. If a 128-bit key is suggested, output it as the user key of the 16-round SMS4; otherwise, go to Step 2-(a).

To get the difference $(0, e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, e_{0,1,\cdots,15})$ just before Round 14 a ciphertext pair must have a difference belonging to Σ_2, and its corresponding plaintext pair must have a difference belonging to Σ_1 to get the difference $(e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, 0)$ just before Round 2, which poses a filtering condition of $\frac{127^6}{2^{64}} \cdot \frac{127^6}{2^{128}} \approx 2^{-108.12}$ over all the ciphertext pairs. There is a filtering condition of $\frac{1}{127}$ in every test of Steps 2-(a), 2-(c), 3-(a) and 3-(c). Therefore, it is expected that only $2^{13.99}$ pairs pass Step 3-(c) for every guess of

$(RK_0, RK_{1,0}, RK_{14,0}, RK_{14,1}, RK_{15})$, and all these remaining pairs have the difference $(0, e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, e_{0,1,\cdots,15})$ just before Round 14. In Step 3-(d), a remaining pair propagates with a probability of $\frac{1}{127}$ to a pair of intermediate values with difference $(e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, 0)$ just after Round 1, thus, we expect with a probability of $\frac{1}{127}$ to get a pair $(S_{i,1}, S_{j,1})$ such that $S_{i,1} \oplus S_{j,1} = \Delta^1_{i,j,1}$, which means the pair has a difference $(e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, e_{0,1,\cdots,15}, 0)$ just after Round 1; however, a subkey guess for which there exists such a pair is impossible. Hence, after analysing all the $2^{13.99}$ remaining ciphertext pairs, only $2^{96} \cdot (1 - 2^{-6.99})^{2^{13.99}} \approx 2^{-88.32}$ possible guesses of the 96 subkey bits pass Step 3-(d). As a result, the expected number of wrong 128-bit keys in Step 4 is about $2^{-128} \cdot 2^{96} = 2^{-32}$, which is extremely low, so we can find the correct 128-bit user key.

The attack requires 2^{105} chosen plaintexts. The time complexity of Steps 2–4 is dominated by the partial encryptions/decryptions in Steps 2-(a), 2-(c), 3-(a), 3-(c) and 3-(d), which is approximately $\sum_{l=1}^{11}(2 \cdot 2^{90.88} \cdot 2^{8 \cdot l} \cdot \frac{1}{127^{l-1}} \cdot \frac{1}{16}) + 2 \cdot 2^{96} \cdot [1 + (1 - 2^{-6.99}) + \cdots + (1 - 2^{-6.99})^{2^{13.99}}] \cdot \frac{1}{16} \approx 2^{107}$ 16-round SMS4 computations.

6 Concluding Remarks

In this paper, we analyse the security of the SMS4 block cipher used in WAPI, a Chinese national standard. We present a rectangle attack on SMS4 reduced to 14 rounds and an impossible differential attack on SMS4 reduced to 16 rounds. These are better than any previously known cryptanalytic results on SMS4 in terms of the numbers of attacked rounds.

Like most cryptanalytic results on block ciphers, our attacks are theoretical in the sense of the assumptions of differential cryptanalysis. We stress that our cryptanalytic attacks do not endanger the full 32 round version of SMS4; the 32 rounds provide a sufficient safety margin against our attacks.

Acknowledgments

The author is very grateful to his supervisor Prof. Chris Mitchell and an anonymous referee for their editorial comments.

References

1. Office of State Commercial Cryptography Administration.: P.R. China, The SMS4 Block Cipher (in Chinese), Archive available at: `http://www.oscca.gov.cn/UpFile/200621016423197990.pdf`
2. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
3. Biham, E., Biryukov, A., Shamir, A.: Miss in the middle attacks on IDEA and Khufu. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 124–138. Springer, Heidelberg (1999)

4. Biham, E., Dunkelman, O., Keller, N.: The rectangle attack — rectangling the Serpent. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 340–357. Springer, Heidelberg (2001)
5. Biham, E., Shamir, A.: Differential cryptanalysis of the Data Encryption Standard. Springer, Heidelberg (1993)
6. The Institute of Electrical and Electronics Engineers (IEEE), http://grouper.ieee.org/groups/802/11
7. International Standardization of Organization (ISO).: International Standard–ISO/IEC 8802-11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39777
8. Kelsey, J., Kohno, T., Schneier, B.: Amplified boomerang attacks against reduced-round MARS and Serpent. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 75–93. Springer, Heidelberg (2001)
9. Knudsen, L.R., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
10. Liu, F., Ji, W., Hu, L., Ding, J., Lv, S., Pyshkin, A., Weinmann, R.P.: Analysis of the SMS4 block cipher. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 158–170. Springer, Heidelberg (2007)
11. Lu, J., Kim, J., Keller, N., Dunkelman, O.: Related-key rectangle attack on 42-round SHACAL-2. In: Katsikas, S.K., Lopez, J., Backes, M., Gritzalis, S., Preneel, B. (eds.) ISC 2006. LNCS, vol. 4176, pp. 85–100. Springer, Heidelberg (2006)
12. Lu, J., Kim, J., Keller, N., Dunkelman, O.: Differential and rectangle attacks on reduced-round SHACAL-1. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 17–31. Springer, Heidelberg (2006)
13. Lu, J., Kim, J., Keller, N., Dunkelman, O.: Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1, Archive available at: http://jiqiang.googlepages.com
14. National Institute of Standards and Technology.: U.S.A., Advanced Encryption Standard (AES) FIPS-197 (2001)
15. Wagner, D.: The boomerang attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)
16. Zhang, L., Wu, W.: Differential fault attack on SMS4 (in Chinese). Chinese Journal of Computers 29(9) (2006)