Improved Linear Cryptanalysis of SMS4 Block Cipher

Joo Yeon Cho[1] and Kaisa Nyberg[2]

[1] Nokia, Denmark
joo.cho@nokia.com
[2] Aalto University and Nokia, Finland
kaisa.nyberg@tkk.fi

Abstract. SMS4 is a block cipher standard used for wireless communications in China. We analyze a reduced versions of SMS4 by the multidimensional linear cryptanalysis method. Our analysis shows that the 23-round of SMS4 can be attacked with $2^{126.6}$ data complexity and time complexity less than exhaustive search.
Keywords : Block Ciphers, Linear Cryptanalysis, SMS4, Multidimensional Linear Cryptanalysis.

1 Introduction

SMS4 is a Chinese block cipher, mandated for use in Wireless LAN WAPI (Wired Authentication and Privacy Infrastructure) [18]. The encryption algorithm written in Chinese was released by the Chinese Government in January 2006 and its English translation was released in 2008 [5].

Once the specification of SMS4 was known in public, several cryptanalysis on SMS4 have been presented in the cryptographic community. An integral attack on 13-round version was first presented in [13] and an algebraic cryptanalysis was presented in [11]. An impossible differential cryptanalysis on 16-round version was performed in [14] and the results were further improved in [17]. Rectangle attacks were applied to 14-round version in [14, 17], 16-round version in [20] and 18-round version in [12]. A boomerang attack on 18-round version was presented in [12]. Differential cryptanalysis was applied to 21-round version in [20] and on 22-round version in [12, 21]. A linear cryptanalysis on 22-round version was presented in [7, 12]. Among these cryptanalyses, the best known attack is the differential attack on the 22-round version of SMS4 which requires 2^{117} data complexity and $2^{112.3}$ time complexity [21].

The linear attack against the 23-round version of SMS4 was also discussed in [7], motivated by the fact that the strongest linear approximation is not single but multiple. However, the result of the discussion was negative and the possibility of the attack was left for future research. Our paper is the response to this open question. We apply the multidimensional linear attack method [9] to SMS4 and show that the 23-round version of SMS4 (out of 32 rounds) can be attacked with less complexity than key exhaustive search.

Multidimensional linear attack [8, 9] is an extension of Matui's linear attack [15], in which maximum 2^m linear approximations can be used for the attack by considering only m-dimensional linear approximations. In this attack, the probability distribution of multidimensional linear approximations is exploited to distinguish the correct key from the wrong keys. The multidimensional linear attack was applied to the block cipher PRESENT [1] up to 26 rounds in [2]. Later in [10], Hermelin and Nyberg proposed an improved algorithm (which is called the *convolution method*) which can reduce the time complexity significantly by applying Fast Walsh-Hadamard Transform algorithm [19].

In this paper, we apply the up-to-date multidimensional linear attack framework to SMS4. Our attack requires $2^{126.7}$ of the data complexity, 2^{127} 23-round encryptions and $2^{120.7}$ memory complexity. Our attack algorithm also demonstrates that the convolution method [10] is highly useful for reducing the time complexity of the attack.

This paper is organized as follows. In Section 2, the algorithm of SMS4 is briefly described and the previous linear attacks are discussed. In Section 3, the multidimensional linear attack methods are presented and an improved technique for reducing the time complexity is presented. In Section 4, the multidimensional linear attack using Algorithm 2 against 23-round version of SMS4 is presented. Section 5 concludes this paper. We also tested the suitability of our attack model for SMS4. In the Appendix we present results from simulations of a multidimensional attack over 8 rounds of the SMS4 cipher.

2 Preliminaries

2.1 Brief Description of SMS4

SMS4 is a generalized Feistel block cipher using a 128-bit key. The encryption algorithm is composed of 32 rounds, each of which takes four 32-bit input words, modifies one of the input words and produces four 32-bit output words including three input words unchanged. Let the 128-bit input block denote the four 32-bit elements (X_0, X_1, X_2, X_3) and $RK_i \in \mathbb{F}_2^{32}$ denote the $(i+1)$-th round key where $0 \leq i \leq 31$. The $(i+1)$-th round function of SMS4 is defined as

$$X_{i+4} = X_i \oplus F(X_{i+1}, X_{i+2}, X_{i+3}, RK_i) = X_i \oplus L(\tau(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus RK_i)) \quad (1)$$

which is illustrated in Figure 1.

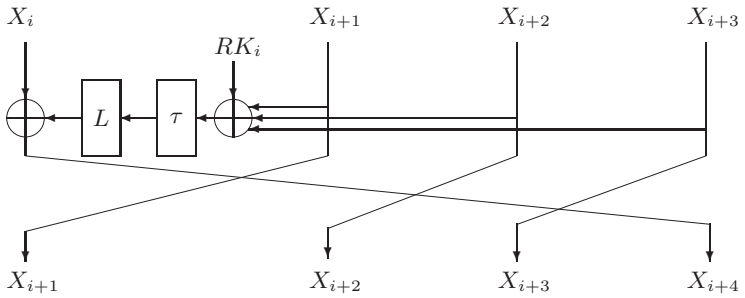

Fig. 1. The i-th round function of SMS4

Both τ and L are described as follows. Let S denote the 8×8 S-box of SMS4. For $A = (a_0, a_1, a_2, a_3) \in (\mathbb{F}_2^8)^4$, the non-linear transformation τ is defined as

$$\tau(A) = S(a_0)||S(a_1)||S(a_2)||S(a_3)$$

where $||$ stands for the concatenation. The linear transformation L is defined as

$$L(X) = X \oplus (X \lll 2) \oplus (X \lll 10) \oplus (X \lll 18) \oplus (X \lll 24)$$

where $X \lll n$ denotes the left-rotated X by n-bit.
Let $(P_0, P_1, P_2, P_3) \in (\mathbb{F}_2^{32})^4$ and $(C_0, C_1, C_2, C_3) \in (\mathbb{F}_2^{32})^4$ be the 128-bit plaintext and ciphertext, respectively. Then, the SMS4 algorithm is described as follows:

1. Set $(X_0, X_1, X_2, X_3) \leftarrow (P_0, P_1, P_2, P_3)$;
2. For $i = 0, 1, \ldots, 31$, do the following
   $X_{i+4} \leftarrow X_i \oplus F(X_{i+1}, X_{i+2}, X_{i+3}, RK_i)$
3. Set $(C_0, C_1, C_2, C_3) \leftarrow (X_{35}, X_{34}, X_{33}, X_{32})$.

Similarly to AES S-box, the S-box of SMS4 is built by the combination of an inverse function and a linear transformation [6]. The encryption and decryption algorithms are identical except that the round keys for decryption are used in the reverse order of the encryption [5]. We omit the key scheduling algorithm here since it is not directly related to our attack. For complete description of SMS4, we refer to the paper [5].

2.2 Previous Linear Cryptanalysis

In this section, we briefly describe the linear cryptanalysis on the 22 rounds version of SMS4 presented in [7]. Let n be a non-negative integer. Given two vectors $a = (a_{n-1}, \ldots, a_0)$ and $b = (b_{n-1}, \ldots, b_0)$, the $a \cdot b$ denotes the standard inner product $a \cdot b = a_{n-1}b_{n-1} \oplus \cdots \oplus a_0 b_0$. Let us consider a function $f : \{0,1\}^n \to \{0,1\}^n$. Given a linear input mask a and an output mask b, the correlation of an approximation $a \cdot x = b \cdot f(x)$ is measured as follows.

$$\rho(a, b) = 2^{-n}(\#(a \cdot x \oplus b \cdot f(x) = 0) - \#(a \cdot x \oplus b \cdot f(x) = 1))$$

where $x \in GF(2^n)$.
Let $\gamma \in \mathbb{F}_2^{32}$ be a linear mask. Equation (1) is linearly approximated by applying γ as both input and output mask as follows:

$$\gamma \cdot X_{i+4} = \gamma \cdot (X_i \oplus X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus RK_i) \tag{2}$$

and the correlation of (2) is denoted as $\rho(\gamma, \gamma)$.
For the next round, we get a similar approximation

$$\gamma \cdot X_{i+5} = \gamma \cdot (X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus X_{i+4} \oplus RK_{i+1}). \tag{3}$$

If (2) and (3) are linearly added, the following approximation is obtained over two rounds:

$$\gamma \cdot (X_i \oplus X_{i+5}) = \gamma \cdot (RK_{i+1} \oplus RK_i) \tag{4}$$

with the correlation of $\rho^2(\gamma, \gamma)$. Note that Approximation (4) is actually built over 5 rounds due to the Feistel structure.
Now, let's consider the 22-round version of SMS4. If we apply Approximation (4) to the fourth and fifth round, then we get

$$\gamma \cdot X_3 \oplus \gamma \cdot X_8 = \gamma \cdot (RK_3 \oplus RK_4). \tag{5}$$

By iterating (5) three times in a serial way and combining them, the following linear approximation is established:

$$\gamma \cdot X_3 \oplus \gamma \cdot X_{18} = \gamma \cdot (RK_3 \oplus RK_4 \oplus RK_8 \oplus RK_9 \oplus RK_{13} \oplus RK_{14}). \tag{6}$$

with the correlation of $\rho^6(\gamma, \gamma)$. Since X_3 is the last input word of the first round and X_{18} is the first output word of the 18-th round, Approximation (6) represents an 18-round linear approximation of SMS4.

In [7], the linear approximations of the single round function were exhaustively searched. In result, 24 linear approximations holding with the highest correlations of $2^{-9.19}$ were identified. Hence, the strongest 18-round linear approximation with a form of (6) has the correlation of $2^{-9.19\times 6} = 2^{-55.14}$. The values of linear masks of the 24 linear approximations are listed in Table 1. In this table, L_2 denotes a transpose function of L. If a is the output mask from L, then the mapping L_2 is defined to satisfy the following equation: $a \cdot L(x) = L_2(a) \cdot x$ for $x \in GF(2^{32})$.

Using 18-round linear approximation (6) which starts from round 3 and ends at the round 20, one can recover 24 bits from both RK_1 and RK_{20} and 32 bits from both RK_0 and RK_{21} by Matsui's algorithm 2 [15]. In [7], the complexity of the linear attack against the 22-round version of SMS4 was estimated with around 2^{118} data complexity and 2^{117} 22-round encryptions.

Discussion Let a be a 32-bit linear mask. Let $\mathcal{A}_0$ be a set of linear masks which is defined as

$$\mathcal{A}_0 = \{a | 0 \le a < 2^{24}, 0 \le L_2(a) < 2^{24}\}.$$

Similarly, $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$ are defined as $\mathcal{A}_i = \{(x \ggg (8 \times i)) | x \in \mathcal{A}_0\}$ for $i = 1, 2, 3$, respectively where $\ggg$ denotes a rotational right shift.

The linear masks in Table 1 have the following properties:

- The linear mask of the best linear approximation is included in one of the $\mathcal{A}_i$ for $i = 0, 1, 2, 3$;
- If $a \in \mathcal{A}_0$, then $\rho(a, a)$ is equal to $\rho(a', a')$ where $a' = (a \ggg (8 \times i))$ for $i = 1, 2, 3$.

Hereafter, we focus on $\mathcal{A}_0$ for further analysis since $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$ are symmetric to $\mathcal{A}_0$.

set	γ	$L_2(\gamma)$	set	γ	$L_2(\gamma)$
	0x0011ffba	0x0084be2f		0xba0011ff	0x2f0084be
	0x007905e1	0x005afbc6		0xe1007905	0xc6005afb
$\mathcal{A}_0$	0x00edca7c	0x0083ffaa	$\mathcal{A}_1$	0x7c00edca	0xaa0083ff
	0x007852b3	0x00582b15		0xb3007852	0x1500582b
	0x00a1b433	0x00f1027a		0x3300a1b4	0x7a00f102
	0x00fa7099	0x00d20b1d		0x9900fa70	0x1d00d20b
	0xffba0011	0xbe2f0084		0x11ffba00	0x84be2f00
	0x05e10079	0xfbc6005a		0x7905e100	0x5afbc600
$\mathcal{A}_2$	0xca7c00ed	0xffaa0083	$\mathcal{A}_3$	0xedca7c00	0x83ffaa00
	0x52b30078	0x2b150058		0x7852b300	0x582b1500
	0xb43300a1	0x027a00f1		0xa1b43300	0xf1027a00
	0x709900fa	0x0b1d00d2		0xfa709900	0xd20b1d00

Table 1. The list of linear masks γ where $\rho(\gamma, \gamma) = 2^{-9.19}$ (This table was taken from [7])

3 Multidimensional Linear Attack

Multidimensional linear cryptanalysis is an extension of Matsui's linear cryptanalysis [15] in which multiple linear approximations are optimally exploited. The general framework of the multidimensional linear cryptanalysis adapting Matsui's algorithm 1 and 2 was presented by Hermelin et al. in [8] and [9].

Let us consider an iterative block cipher which maps a plaintext P to a ciphertext C with a secret key K. Suppose we choose a set of m linear independent approximations $f_0, \cdots, f_{m-1}$ where each f_i is represented by

$$U_i \cdot P \oplus V_i \cdot C = W_i \cdot K, \quad 0 \le i \le m-1$$

where U_i, V_i and W_i denote the linear masks. The number of possible linear combinations of $f_0, \cdots, f_{m-1}$ is $2^m - 1$. The multidimensional linear attack allows us to use the capability of $2^m - 1$ linear approximations by evaluating only m linearly independent approximations. The $f_0, \cdots, f_{m-1}$ are called *base approximations* and the correlations of linear combinations of base approximations are denoted by $c_1, \cdots, c_{2^m-1}$.

Let G denote the m-bit vector as $G = (g_0, \ldots, g_{m-1}) \in \mathbb{F}_2^m$ where $g_i = W_i \cdot K$. Then, for a fixed G, the probability distribution p_G of the m-dimensional linear approximation is built as $p_G = (p_{0,G}, \ldots, p_{2^m-1,G})$ where

$$p_{i,G} = 2^{-m} \sum_{j=0}^{2^m-1} (-1)^{j \cdot (i \oplus G)} c_j \tag{7}$$

with the assumption of $c_0 = 1$. In [9], the log-likelihood ratio (LLR) statistic is used for the optimal distinguisher between two probability distribution p and q as follows:

$$LLR(p, q) = \sum_{i=0}^{2^m-1} q_i \log \frac{p_i}{u_i} = \sum_{i=0}^{2^m-1} q_i \log p_i + m. \tag{8}$$

where $u = (u_0, \ldots, u_{2^m-1})$ is the uniform distribution. The capacity of the probability distribution p_G is defined as $C_p = 2^m \sum_{i=0}^{2^m-1} (p_{i,G} - 2^{-m})^2$. It is known that the C_p is equal to the sum of the square of correlations of all $2^m - 1$ linear approximations [4].

Multidimensional Algorithm 1 (MA1) MA1 attack targets to recover the m parity bits of the key by using the m-dimensional linear approximation. In the preprocessing phase, the attacker constructs the probability distribution $p_G = (p_{0,G}, \ldots, p_{2^m-1,G})$ for each possible value of G by (7). Since there are 2^m possible values for G, the attacker needs to store the probability distribution table which has $2^m \times 2^m$ entries. In the processing phase, the attacker collects the sufficient number of plaintext-ciphertext pairs generated with the unknown key K and computes the empirical probability distribution $q_K = (q_{0,K}, \ldots, q_{2^m-1,K})$ by measuring the frequency of the vectors $(g_0, \ldots, g_{m-1}) \in \mathbb{F}_2^m$ where $g_i = U_i \cdot P \oplus V_i \cdot C$. Among the possible candidates of G, the correctly guessed candidate is likely to have the maximum log-likelihood ratio to the uniform distribution. Hence, the attacker choose the G such that $\max_G LLR(p_G, q_K)$ as the right key.

Multidimensional Algorithm 2 (MA2) MA2 can be seen as an extended Matsui's algorithm 2 which nests MA1; the attacker guesses the parts of the round keys in the first and

last rounds, and proceeds the MA1 attack over the remaining rounds with the m-dimensional linear approximation. Suppose l is the length of the guessed key in the first and last rounds. The attacker retrieves the empirical probability distribution $q_\kappa = (q_{\kappa,0}, \ldots, q_{\kappa,2^m-1})$ for each possible value of $\kappa \in [0, 2^l - 1]$. Then, the attacker choose κ and G such that $\max_\kappa \max_G LLR(p_G, q_\kappa)$ as the right key values. Hence, the attacker can recover $(l + m)$ bits information of the secret key.

Reducing Time Complexity In [10], Hermelin et al. proposed an improved algorithm (which is called the *convolution method*) which can reduce the time complexity of the attack significantly. The details are as follows. According to the MA1, the LLR-statistic needs to be computed for all possible values of $G \in GF(2^m)$ and each LLR-statistic needs 2^m operations. Hence, the MA1 attack requires around $2^m \cdot 2^m$ on-line computation efforts, which is the major bottleneck of the multidimensional linear attack method.

This complexity can be greatly reduced by using Fast Walsh Hadamard Transform [19]. Instead of using LLR-statistics, the statistical decision can be equivalently made by computing

$$D_G = \sum_{i=0}^{2^m-1} (-1)^{i \oplus G} \hat{c_i} \times c_i \tag{9}$$

where $\hat{c_0}, \ldots, \hat{c_{2^m-1}}$ are the empirically measured correlations of $2^m - 1$ linear approximations [10]. Hence, we do not need to store the $2^m \times 2^m$ size of the probability distribution table; we need to store $c_1, \ldots, c_{2^m-1}$, or more practically we need to store only the significant correlations among $2^m - 1$ correlations. Then (9) can be efficiently computed by Fast Walsh Hadamard Transform which requires $m \times 2^m$ operations. The correct key is recovered by choosing G such that D_G is maximal. We note that D_G is independent of G due to Equation (8).

Let l be the length of the guessed key. Since the D_G is computed for each key candidate, the required computations are reduced to $m \cdot 2^m \cdot 2^l$. Let k be the total key length (for SMS4, $k = 128$). In order to be faster than the key exhaustive search, MA1 and MA2 should satisfy the following conditions:

Condition for MA1: $m \cdot 2^m < 2^k \Longleftrightarrow \log_2(m) + m < k$

Condition for MA2: $m \cdot 2^m \cdot 2^l < 2^k \Longleftrightarrow \log_2(m) + m + l < k$

In Section 4.3, we apply MA2 attack to the 23-round version of SMS4 with the parameter of $m = 34$ and $l = 88$.

4 Multidimensional Linear Attack on SMS4

4.1 Correlation of $\rho(\gamma, \gamma)$

Let us recall Section 2.2. Apart from the linear approximations listed in Table 1, we observe that there are 52744 non-zero linear approximations in $\mathcal{A}_0$. The number of linear approximations from the strongest one is displayed in Table 2. Furthermore, we observe that all the non-zero approximations can be generated by using 16 base approximations listed in Table 5 even though the number of "active" bits in $\mathcal{A}_0$ is 24.

Let's consider an 8-round linear characteristic which uses the linear approximation of (5). According to Table 1, the strongest approximation of (5) holds with the correlation of

$(2^{-9.19})^2 = 2^{-18.38}$. Hence, Matsui's linear attack using a single linear approximation requires around $(2^{-18.38})^{-2} = 2^{36.76}$ data complexity. On the contrary, the multidimensional linear attack can take these 16 base approximations and use the capacity of those probability distribution. Computation shows that the capacity is around $2^{-29.3}$.

Let $\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt$ be the normal cumulative distribution function. In [8], the data complexity for MA1 is calculated as

$$N_{MA1} = \frac{(\Phi^{-1}(P_S) + \Phi^{-1}(1 - 2^{-a}))^2}{C_p}$$

where P_S stands for a success probability, C_p means a capacity and a denotes the advantage of the attack. We say that the attack has the advantage of $a = (m - \log_2 d)$ if the right key is ranked in the position of d from the top out of 2^m key candidates [16]. Hence, the full advantage ($a = 16$) can be achieved with the data complexity of around $2^{34.4}$.

We verified our estimation by experiment. We applied the MA1 attack to 8 rounds of SMS4. See Appendix A. Figure 2 shows that the experimental result is well matched with the theoretical estimation.

$\lvert\rho(\gamma,\gamma)\rvert$	Number of approx.	$\lvert\rho(\alpha,\gamma)\rvert$	Number of approx.
$2^{-9.19}$	6	$2^{-9.0}$	125
$2^{-9.39}$	11	$2^{-9.10}$	0
$2^{-9.42}$	15	$2^{-9.20}$	1200
$2^{-9.58}$	12	$2^{-9.30}$	0
$2^{-9.61}$	76	$2^{-9.40}$	6540
$2^{-9.68}$	7	$2^{-9.50}$	0
$2^{-9.80}$	120	$2^{-9.60}$	21376
$2^{-9.83}$	89	$2^{-9.70}$	1800
$2^{-9.87}$	56	$2^{-9.80}$	47088

Table 2. Evaluation of the number of linear approximations of the round function where $\gamma \in \mathcal{A}_0$

4.2 Correlation of $\rho(\alpha, \gamma)$

Suppose $\gamma \in \mathcal{A}_0$ is one of the linear masks which are listed in Table 1. We observe that, for $0 \leq \alpha \leq 2^{24}$, the strongest value of $\rho(\alpha, \gamma)$ is $2^{-9.0}$ and $\#\{\alpha | \rho(\alpha, \gamma) = 2^{-9.0}\} = 125$. The partial list on the number of linear approximations is displayed in the right side of Table 2.

4.3 MA2 Attack on 23-round SMS4

In this attack, we build a 20-round linear characteristic which starts from round 3 and ends at round 22. Then, we apply MA2 attack for recovering 88 bits of round key (32 bits of RK_0, 32 bits of RK_1 and 24 bits of RK_{22}) and 34 parity bits of round keys.

20-Round Linear Characteristic Let $\alpha, \beta, \gamma \in GF(2^{32})$ be linear masks where $\alpha, \beta, \gamma \in \mathcal{A}_i$ for $i = 0, 1, 2, 3$. First, we build two rounds characteristic using α, β and γ in round 3

and 4 as follows:

$$\begin{aligned}\alpha \cdot X_2 \oplus \beta \cdot (X_3 \oplus X_4 \oplus X_5 \oplus RK_2) &= \alpha \cdot X_6 \\ \gamma \cdot X_3 \oplus \alpha \cdot (X_4 \oplus X_5 \oplus X_6 \oplus RK_3) &= \gamma \cdot X_7 \end{aligned} \tag{10}$$

Then, the correlation of (10) is $\rho(\beta,\alpha)\rho(\alpha,\gamma)$. From round 8 to round 22, we use the 15-round characteristic which is of the form (6).

$$\gamma \cdot X_7 \oplus \gamma \cdot X_{22} = \gamma \cdot (RK_7 \oplus RK_8 \oplus RK_{12} \oplus RK_{13} \oplus RK_{17} \oplus RK_{18}) \tag{11}$$

Then, by combining (10) and (11), we get

$$\begin{aligned}&\alpha \cdot X_2 \oplus (\beta \oplus \gamma) \cdot X_3 \oplus (\alpha \oplus \beta) \cdot (X_4 \oplus X_5) \oplus \gamma \cdot X_{22} \\ &= \beta \cdot RK_2 \oplus \alpha \cdot RK_3 \oplus \gamma \cdot (RK_7 \oplus RK_8 \oplus RK_{12} \oplus RK_{13} \oplus RK_{17} \oplus RK_{18}) \end{aligned} \tag{12}$$

with the correlation of $\rho(\beta,\alpha)\rho(\alpha,\gamma)\rho^6(\gamma,\gamma)$. The left part of the characteristic (12) can be expressed as

$$(\alpha, \beta \oplus \gamma, \alpha \oplus \beta, \alpha \oplus \beta) \cdot P \oplus (\gamma, 0, 0, 0) \cdot C$$

where $P = (X_2, X_3, X_4, X_5)$ and $C = (X_{22}, X_{23}, X_{24}, X_{25})$. Note that another linear characteristic with an equivalent correlation can be built by moving the two rounds characteristic (10) to the last two rounds. 20-round characteristics are further discussed in Appendix B.

Probability Distribution and Capacity Let $\gamma \in \mathcal{A}_0$. Since the most significant 8 bits are zero and $0 \le L_2(\gamma) < 2^{24}$, it is sufficient to guess the lower 24 bits for RK_{22}. We assume that $0 \le \alpha \le 2^{24}$. Since $0 \le L_2(\alpha) < 2^{32}$, it is needed that $0 \le \beta \le 2^{32}$. Hence, the full length of round key (32 bits) for RK_0 and RK_1 should be guessed. Therefore, the target key length is $32 \cdot 2 + 24 = 88$ bits.

Let m be the number of base approximations over the 20-round characteristic (12). We apply the convolution method [10] to build the probability distribution of m approximations. Suppose that δ is a threshold value which determines the number of linear approximations being used for an attack. Let us define $\mathcal{M}$ as

$$\mathcal{M} = \{(\alpha,\beta) \mid (\rho(\beta,\alpha)\rho(\alpha,\gamma))^2 > \delta\}.$$

Then, the capacity of the probability distribution is calculated as

$$C_p = \sum_{\gamma \in \mathcal{A}_0} C_{\mathcal{M}}(\gamma) \tag{13}$$

where

$$C_{\mathcal{M}}(\gamma) = \sum_{(\alpha,\beta)\in\mathcal{M}} \rho^2(\beta,\alpha)\rho^2(\alpha,\gamma)\rho^{12}(\gamma,\gamma). \tag{14}$$

We denote $M = |\mathcal{M}|$. The capacities of multiple approximations for several values of M are evaluated in Table 3 when $\rho(\gamma,\gamma) = 2^{-9.19}$ is used. Then, we need to determine the minimum dimension m of base approximations which can span M linear approximations whose capacity is sufficient for the attack. As described in Section 3, m should satisfy the condition that $\log_2(m) + m + 88 < 128$, that is, $m \le 34$.

We searched exhaustively the base approximations which yield the maximum capacity. We could not finish searching for all combinations of the possible base approximations. So far, we found that 34 base approximations could span an sufficient number of non-negligible linear approximations. It would be an interesting research topic how to find the best base approximations efficiently. We also note that the multiple linear approximations in $\mathcal{A}_1$, $\mathcal{A}_2$ and $\mathcal{A}_3$ can be also used for the attack since they are symmetrical to $\mathcal{A}_0$.

δ	M	C_p
$2^{-36.0}$	$125 = 2^{7.0}$	$2^{-135.6}$
$2^{-36.4}$	$2075 = 2^{11.0}$	$2^{-131.9}$
$2^{-36.8}$	$14615 = 2^{13.8}$	$2^{-129.5}$
$2^{-37.2}$	$62476 = 2^{15.9}$	$2^{-127.7}$
$2^{-37.6}$	$211462 = 2^{17.7}$	$2^{-126.2}$
$2^{-38.0}$	$1696134 = 2^{20.7}$	$2^{-123.0}$
$2^{-38.4}$	$4249383 = 2^{22.0}$	$2^{-122.0}$
$2^{-38.8}$	$10655129 = 2^{23.4}$	$2^{-121.3}$
$2^{-39.2}$	$31530029 = 2^{24.7}$	$2^{-119.7}$
$2^{-39.6}$	$75192630 = 2^{26.2}$	$2^{-119.0}$

Table 3. Evaluation of the number of linear approximations and capacity when $\rho(\gamma, \gamma) = 2^{-9.19}$

Attack Algorithm Let N_{MA2} denote the data complexity required for the MA2 attack. Under the Matsui's algorithm 2 attack scenario, we perform the 2-round encryption and 1-round decryption on each plaintext-ciphertext pair per each guessed key, which requires $O(N_{MA2} \cdot 2^l)$ time complexity for a naive implementation. Since this step includes many repeated computations, we can reduce the time complexity by dividing this step into two sub steps: first, we store the relevant parts of the plaintext-ciphertext pairs in the memory, and later we calculate the desired correlations from the stored values by Fast Fourier Transform. This technique was presented by Collard et al. in [3] and applied to 22-round version of SMS4 by Etrog et al. in [7].

Let us denote $T_0 = X_1 \oplus X_2 \oplus X_3$, $T_1 = X_0 \oplus X_2 \oplus X_3$ $T_2 = X_{23} \oplus X_{24} \oplus X_{25}$. By the definition of the round function, we can write

$$\begin{aligned} &X_0 \oplus F(T_0 \oplus RK_0) = X_4, \\ &X_1 \oplus F(T_1 \oplus F(T_0 \oplus RK_0) \oplus RK_1) = X_5 \text{ and} \\ &X_{26} \oplus F(T_2 \oplus RK_{22}) = X_{22}. \end{aligned}$$

Then, the left side of (12) is transformed into

$$\begin{aligned} &\alpha \cdot X_2 \oplus (\beta \oplus \gamma) \cdot X_3 \oplus (\alpha \oplus \beta) \cdot (X_0 \oplus X_1) \oplus \gamma \cdot X_{26} \\ &\gamma \cdot F(T_2 \oplus RK_{22}) \oplus (\alpha \oplus \beta) \cdot (F(T_0 \oplus RK_0) \oplus F(T_1 \oplus F(T_0 \oplus RK_0) \oplus RK_1)) \end{aligned}$$

where $(\alpha, \beta) \in \mathcal{M}$.

In the preprocessing phase, MA2 attack proceeds the following steps:

1. Choose m base approximations $f_1, , f_m$ and index their 2^m linear combinations $a_1 f_1 \oplus \cdots \oplus a_m f_m$ using m-bit integers $(a_1, \ldots, a_m)$. From them, choose a subset I of size M consisting of indices of those linear approximations that have significant correlations.
2. Calculate the correlation of linear approximations by using the linear correlation table of the S-box and store c_i, $i \in I$.

In the Online phase, we proceed along the following

1. Prepare $M \times 2^{96}$ counters $w[i][0], \ldots, w[i][2^{96} - 1]$ where $i \in I$. Initialize all counters to zeros.
2. Collect the N_{MA2} plaintext-ciphertext pairs of 23-round SMS4.

3. Let $x \in \mathbb{F}_2$ be defined as
$$x = \alpha \cdot X_2 \oplus (\beta \oplus \gamma) \cdot X_3 \oplus (\alpha \oplus \beta) \cdot (X_0 \oplus X_1) \oplus \gamma \cdot X_{26}.$$
Compute x for all plaintext-ciphertext pairs and all linear approximations. If $x = 0$, increment the counter $w[i][t]$ where $t = (T_0||T_1||T_2) \in \mathbb{F}_2^{96}$ and $i \in I$.
4. Let us denote $k = RK_0||RK_1||RK_{22} \in \mathbb{F}_2^l$. We define $\sigma_{t,k}$ as
$$\sigma(t,k) = \gamma \cdot F(T_2 \oplus RK_{22}) \oplus (\alpha \oplus \beta) \cdot (F(T_0 \oplus RK_0) \oplus F(T_1 \oplus F(T_0 \oplus RK_0) \oplus RK_1)).$$
For a fixed k, compute the empirical correlations $\hat{c}_{0,k}, \ldots, \hat{c}_{M-1,k}$ by the Fast Fourier Transform as
$$\hat{c}_{i,k} = \frac{1}{N_{MA2}} \sum_{t=0}^{2^{96}-1} (-1)^{\sigma(t,k)} w[i][t], \quad i \in I.$$
5. For all possible values of G, compute $D_{k,G}$ such that
$$D_{k,G} = \sum_{i \in I} (-1)^{i \oplus G} \hat{c}_{i,k} \times c_i$$
where $\hat{c}_{I,k} = c_i = 0$, for $i \notin I$.
6. Choose k and G such that $\max_k \max_G D_{k,G}$ is achieved. Then G determines m bits of information of the right hand side of (12) where (α, β, γ) are the mask values for the base approximations $f_1, \ldots, f_m$.

Complexity Let a be the advantage of the attack. According to [8], the data complexity required for MA2 attack is
$$N_{MA2} = \frac{(\Phi^{-1}(P_S) + \Phi^{-1}(1 - 2^{-m-a}))^2}{C_p} \approx \frac{(l+m)}{C_p} \tag{15}$$
where P_S is a success probability and Φ is the cumulative distribution function. We chose $m = 34$ and $M = 2^{24.7}$. Then, the capacity of the 20-round characteristic (12) is $C_p = 2^{-119.7}$ and the data complexity required for the full advantage ($a = 88$) of the attack is around $N_{MA2} = (88 + 34)/2^{-119.7} = 2^{126.6}$ with $Ps = 0.95$.

The computational efforts is estimated as follows. In the Step 3, we need evaluate M linear approximations. This step can be done efficiently by evaluating the base approximations at first and combing them later, which requires around $N_{MA2} \cdot m$ computations. The Step 4 can be done by Fast Fourier Transform which requires around $3 \cdot 96 \cdot 2^{96} \cdot M$. The Step 5 is performed for each key by Fast Walsh Transform, which requires around $34 \cdot 2^{34} \cdot 2^{88} = 2^{127.0}$. In total, the work efforts for Step 3 - 5 can be estimated as $(2^{126.6} \cdot 34 + 3 \cdot 96 \cdot 2^{96} \cdot 2^{24.7} + 2^{126.4})/23 \approx 2^{127.4}$ 23-round encryptions. The memory requirement is $M \cdot 2^{96} + 3 \cdot 2^{96} \approx 2^{120.7}$. The remaining key bits $(128 - 88)$ can be recovered by exhaustive search.

We summarize our new attacks and selected previously published attacks against the reduced-round version of SMS4 in Table 4.

5 Conclusion

In this paper, we showed how the multidimensional linear cryptanalysis could improve the previous linear attack on the reduced version of SMS4. We adapted a recently developed multidimensional attack technique using Fast Walsh Transform for the linear attack on the reduced version of SMS4. We showed that the work efforts for computing the statistic distinguisher could be reduced. We should note that there is still a room for improving the performance of the attack. We leave this issue for future research.

round	data	time	memory	method
22	$2^{118.4}$	2^{117}	2^{112}	Linear [7]
22	2^{117}	$2^{112.3}$	2^{110}	Differential [21]
23	$2^{126.6}$	$2^{127.4}$	$2^{120.7}$	MultiDim. Linear (this paper)

Table 4. Comparison of data and time complexity of the attacks against reduced-round SMS4

References

1. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*, Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings, Lecture Notes in Computer Science, vol. 4727, Springer, 2007, pp. 450–466.
2. J. Cho, *Linear cryptanalysis of reduced-round present*, Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings, Lecture Notes in Computer Science, vol. 5985, Springer, 2010, pp. 302–317.
3. B. Collard, F. Standaert, and J. Quisquater, *Improving the time complexity of Matsui's linear cryptanalysis*, Information Security and Cryptology - ICISC 2007, 10th International Conference, Seoul, Korea, November 29-30, 2007, Proceedings, Lecture Notes in Computer Science, vol. 4817, Springer, 2007, pp. 77–88.
4. J. Daemen and V. Rijmen, *The Design of Rijndael- AES, the Advanced Encryption Standard*, Springer-Verlag, 2002.
5. W. Diffie and G. Ledin (translators), *SMS4 encryption algorithm for wireless networks*, Cryptology ePrint Archive, Report 2008/329, 2008, http://eprint.iacr.org/2008/329.
6. J. Erickson, *Algebraic cryptanalysis of SMS4*, Available at www.nku.edu/ christensen/SMS4%20jeremy.pdf.
7. J. Etrog and M. Robshaw, *The cryptanalysis of reduced-round sms4*, Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers, vol. 5381, 2008, pp. 51–65.
8. M. Hermelin, J. Y. Cho, and K. Nyberg, *Multidimensional linear cryptanalysis of reduced round Serpent*, Information Security and Privacy, 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings, Lecture Notes in Computer Science, vol. 5107, Springer, 2008, pp. 203–215.
9. ———, *Multidimensional extension of Matsui's algorithm 2*, Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers, Lecture Notes in Computer Science, vol. 5665, Springer, 2009, pp. 209–227.
10. M. Hermelin and K. Nyberg, *Dependent linear approximations: The algorithm of biryukov and others revisited*, Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings, Lecture Notes in Computer Science, vol. 5985, Springer, 2010, pp. 318–333.
11. W. Ji and L. Hu, *New description of SMS4 by an embedding over* $GF(2^8)$, Progress in Cryptology - INDOCRYPT 2007, 8th International Conference on Cryptology in India, Chennai, India, December 9-13, 2007, Proceedings, Lecture Notes in Computer Science, vol. 4859, Springer, 2007, pp. 238–251.
12. T. Kim, J. Kim, S. Hong, and J. Sung, *Linear and differential cryptanalysis of reduced SMS4 block cipher*, Cryptology ePrint Archive, Report 2008/281, 2008, http://eprint.iacr.org/.
13. F. Liu, W. Ji, L. Hu, J. Ding, S. Lv, A. Pyshkin, and R. Weinmann, *Analysis of the SMS4 block cipher*, Information Security and Privacy, 12th Australasian Conference, ACISP 2007, Townsville, Australia, July 2-4, 2007, Proceedings, Lecture Notes in Computer Science, vol. 4586, Springer, 2007, pp. 158–170.
14. J. Lu, *Attacking reduced-round versions of the SMS4 block cipher in the Chinese WAPI standard*, Information and Communications Security, 9th International Conference, ICICS 2007,

Zhengzhou, China, December 12-15, 2007, Proceedings, Lecture Notes in Computer Science, vol. 4861, Springer, 2007, pp. 306–318.
15. M. Matsui, *Linear cryptoanalysis method for DES cipher*, Advances in Cryptology - EUROCRYPT '93, Lecture Notes in Computer Science, vol. 765, Springer, 1993, pp. 386–397.
16. A. Selçuk, *On probability of success in linear and differential cryptanalysis*, Journal of Cryptology **21** (2008), no. 1, 131–147.
17. D. Toz and O. Dunkelman, *Analysis of two attacks on reduced-round versions of the SMS4*, Information and Communications Security, 10th International Conference, ICICS 2008, Birmingham, UK, October 20-22, 2008, Proceedings, Lecture Notes in Computer Science, vol. 5308, Springer, 2008, pp. 141–156.
18. Wikipedia, *SMS4*, Available at http://en.wikipedia.org/wiki/SMS4.
19. R. K. Yarlagadda and J.E. Hershey, *Hadamard Matrix Analysis and Synthesis: With applications to communications and signal/image processing*, Kluwer Academic Publishers, Norwell, MA, USA, 1997.
20. L. Zhang, W. Zhang, and W. Wu, *Cryptanalysis of reduced-round SMS4 block cipher*, Information Security and Privacy, 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings, Lecture Notes in Computer Science, vol. 5107, Springer, 2008, pp. 216–229.
21. W. Zhang, W. Wu, D. Feng, and B. Su, *Some new observations on the SMS4 block cipher in the Chinese WAPI Standard*, Information Security Practice and Experience, 5th International Conference, ISPEC 2009, Xi'an, China, April 13-15, 2009, Proceedings, Lecture Notes in Computer Science, vol. 5451, Springer, 2009, pp. 324–335.

A MA1 Attack against 8-round SMS4

In this section, we demonstrate how the multidimensional linear attack can improve Matsui's linear attack using a single linear approximation. Due to the restriction of computational resource, we target to recover 16 parity bits of round keys by applying the MA1 attack against an 8-round version of SMS4. In [7], it is reported that the best 8-round linear characteristic (5) holds with the correlation of $2^{-18.4}$. Hence, Matsui's Algorithm 1 attack using this single approximation requires around $2^{36.8}$ data complexity.

Let us assume that $B = \{a|\rho(a, a) \neq 0\}$. We found that there exist many linear approximations which have non-negligible correlation in the set B. If we take sixteen base approximations, we can use 52744 non-zero linear approximations. By computer simulation, we found that the capacity grew up to $2^{-29.3}$.

We performed the Algorithm 1 attack and compared the result with the theoretical estimation in Figure 2. The experiment was repeated 30 times with randomly chosen keys and the average of the advantage was computed. The solid line indicates the empirical result and the dot line indicates the theoretical estimation. The graphs show that our estimation is well matched with the real attack.

B Other 20-round linear chracteristics

Other 20-Round Linear Characteristic We can build other forms of 20-round linear characteristics which have equivalent correlations with (12). First, we derive a single linear characteristic for round 3 by using α and γ as follows:

$$\gamma \cdot X_2 \oplus \alpha \cdot (X_3 \oplus X_4 \oplus X_5 \oplus RK_2) = \gamma \cdot X_6 \tag{16}$$

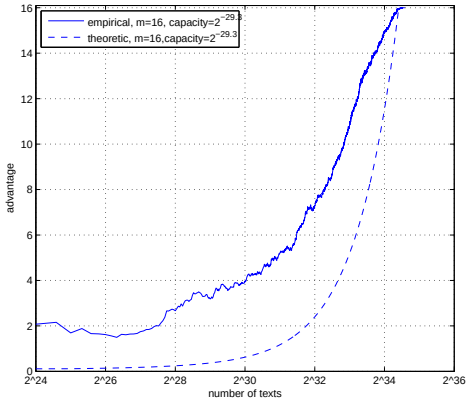

Fig. 2. Comparison of empirical results and theoretical estimation on the linear attack of 8-round SMS4

index	mask	$\rho(\gamma, \gamma)$
1	0x0011ffba	$2^{-9.2}$
2	0x007905e1	$2^{-9.2}$
3	0x00edca7c	$2^{-9.2}$
4	0x007852b3	$2^{-9.2}$
5	0x00a1b433	$2^{-9.2}$
6	0x00fa7099	$2^{-9.2}$
7	0x001390df	$2^{-9.4}$
8	0x001ddeab	$2^{-9.4}$
9	0x00309757	$2^{-9.4}$
10	0x003461b1	$2^{-9.4}$
11	0x0038a545	$2^{-9.4}$
12	0x003faa55	$2^{-9.4}$
13	0x0041b3b7	$2^{-9.4}$
14	0x004da296	$2^{-9.4}$
15	0x0062a12a	$2^{-9.4}$
16	0x007019d8	$2^{-9.4}$

Table 5. Linear masks of the base approximation for 8-round characteristic

with the correlation of $\rho(\alpha, \gamma)$. Next, we reuse the 18-round characteristic of (6) from round 7 to round 21. Then, we get

$$\gamma \cdot X_6 \oplus \gamma \cdot X_{21} = \gamma \cdot (RK_6 \oplus RK_7 \oplus RK_{11} \oplus RK_{12} \oplus RK_{16} \oplus RK_{17}) \tag{17}$$

with the correlation of $\rho^6(\gamma, \gamma)$. Finally, we derive a single round linear characteristic using γ and β for round 22 as follows:

$$\gamma \cdot X_{21} \oplus \beta \cdot (X_{22} \oplus X_{23} \oplus X_{24} \oplus RK_{21}) = \gamma \cdot X_{25} \tag{18}$$

holding with the correlation of $\rho(\beta, \gamma)$.

In result, the combination of (16), (17) and (18) gives us the following 20-round linear characteristic:

$$\begin{aligned} &\gamma \cdot X_2 \oplus \alpha \cdot (X_3 \oplus X_4 \oplus X_5) \oplus \beta \cdot (X_{22} \oplus X_{23} \oplus X_{24}) \oplus \gamma \cdot X_{25} \\ &= \alpha \cdot RK_2 \oplus \gamma \cdot (RK_6 \oplus RK_7 \oplus RK_{11} \oplus RK_{12} \oplus RK_{16} \oplus RK_{17})) \oplus \beta \cdot RK_{21} \end{aligned} \tag{19}$$

and the correlation of (19) is $\rho(\alpha, \gamma)\rho^6(\gamma, \gamma)\rho(\beta, \gamma)$.

Apart from (19) and (12), another form of 20-round characteristic can be built as follows. First, we use a single characteristic (16) in the round 3.

$$\gamma \cdot X_2 \oplus \alpha \cdot (X_3 \oplus X_4 \oplus X_5 \oplus RK_2) = \gamma \cdot X_6$$

Second, instead of using (17), we derive

$$\begin{aligned} &\gamma \cdot X_5 \oplus \gamma \cdot (X_6 \oplus X_7 \oplus X_8 \oplus RK_5) = \gamma \cdot X_9 \\ &\gamma \cdot X_7 \oplus \gamma \cdot (X_8 \oplus X_9 \oplus X_{10} \oplus RK_7) = \gamma \cdot X_{11} \\ &\gamma \cdot X_{10} \oplus \gamma \cdot (X_{11} \oplus X_{12} \oplus X_{13} \oplus RK_{10}) = \gamma \cdot X_{14} \\ &\gamma \cdot X_{12} \oplus \gamma \cdot (X_{13} \oplus X_{14} \oplus X_{15} \oplus RK_{12}) = \gamma \cdot X_{16} \\ &\gamma \cdot X_{15} \oplus \gamma \cdot (X_{16} \oplus X_{17} \oplus X_{18} \oplus RK_{15}) = \gamma \cdot X_{19} \\ &\gamma \cdot X_{17} \oplus \gamma \cdot (X_{18} \oplus X_{19} \oplus X_{20} \oplus RK_{17}) = \gamma \cdot X_{21} \\ &\gamma \cdot X_{20} \oplus \gamma \cdot (X_{21} \oplus X_{22} \oplus X_{23} \oplus RK_{20}) = \gamma \cdot X_{24} \end{aligned}$$

Then, by combining them, we get

$$\begin{aligned} &\gamma \cdot X_2 \oplus \alpha \cdot (X_3 \oplus X_4) \oplus (\alpha \oplus \gamma) \cdot X_5 \oplus \gamma \cdot (X_{22} \oplus X_{23} \oplus X_{24}) = \\ &\alpha \cdot RK_2 \oplus \gamma \cdot (RK_5 \oplus RK_7 \oplus RK_{10} \oplus RK_{12} \oplus RK_{15} \oplus RK_{17} \oplus RK_{20}) \end{aligned}$$

with the correlation of $\rho(\alpha, \gamma)\rho^7(\gamma, \gamma)$.