The Cryptanalysis of Reduced-Round SMS4

Jonathan Etrog* and M.J.B. Robshaw

Orange Labs
38–40 rue du Général Leclerc
92794 Issy les Moulineaux Cedex 9, France
{forename.surname}@orange-ftgroup.com

Abstract In this paper we consider the cryptanalysis of the block cipher SMS4. The cipher has received much recent attention due its simplicity and prominence (it is used in wireless networks in China) and a range of differential attacks break up to 21 of the 32 rounds used in SMS4. Here we consider the application of linear cryptanalysis to the cipher and we demonstrate a simple attack on 22 rounds of SMS4. We also consider some advanced linear cryptanalytic techniques which, under the best conditions for the cryptanalyst, might (just) extend to 23 rounds.

1 Introduction

In this paper we consider the security of the block cipher SMS4 which is reputedly mandated for wireless networks in China [10]. A Chinese description of the cipher was made public in 2006 by the Chinese government, and the first analysis in the open community was published in 2007 [10]. The cipher takes a 128-bit block and key, and it consists of 32 simple rounds. Its intriguing design encourages analysis; something which is due in no small part to the fact that minor variants of the cipher are exceptionally weak.

The first open analysis of a reduced-round version of SMS4 examined the algebraic nature of the algorithm—thereby uncovering the construction of the S-box—and yielded a saturation attack over 13 rounds using 2^{16} chosen plaintext pairs and 2^{114} operations [10]. This was followed by a differential attack on 14 rounds and then by an impossible differential attack on 16 rounds with the claimed requirements of 2^{105} chosen plaintext pairs and 2^{107} operations [11]. These are rather complex attacks, and a more natural differential attack has been revealed that suggests that 21 rounds could be compromised using 2^{118} chosen plaintext pairs and $2^{126.6}$ operations [22]. This is the previous best known attack in the literature.

In this paper we present the first reported application of linear cryptanalysis to SMS4. Apart from DES [15], there are few ciphers for which linear cryptanalysis yields a more efficient attack than differential cryptanalysis. However, for SMS4 we propose an attack on 22 rounds of the cipher with less than 2^{119} known plaintexts and a work effort roughly equivalent to 2^{117} 22-round SMS encryptions. The attack can be clearly described and the necessary components have

* Partially supported by the national research project RFIDAP ANR-08-SESU-009-03.

Appeared in : SAC 2008, LCNS , pp. 0–,

been experimentally verified. We also consider attacks on 23 rounds of SMS4 and highlight some future research directions.

2 Description of SMS4

We briefly describe the block cipher SMS4, but first we establish our notation.

Notation. For the most part we will be working with 32-bit words, though the context will be clear when we restrict ourselves to bytes. The left rotation (*resp.* right rotation) of a word x by b bit positions will be denoted $x \lll b$ (*resp.* $x \ggg b$). The remaining notation is standard in the cryptographic literature.

Encryption and decryption. SMS4 is a 32-round block cipher with a 128-bit key and block. It is an unbalanced Feistel cipher, that repeatedly uses an 8-bit S-box S. This is described in the appendices and it is, by way of construction [10], closely related to the AES S-box [16]. We define the L function and the γ function as follows

$$L(x) = x \oplus (x \lll 2) \oplus (x \lll 10) \oplus (x \lll 18) \oplus (x \lll 24)$$
$$\gamma(x) = (S[x_{31\ldots24}] \,||\, S[x_{23\ldots15}] \,||\, S[x_{15\ldots8}] \,||\, S[x_{7\ldots0}]).$$

The action of the round function f on input X_{i-1} to the i^{th} round of SMS4 is given by $f(X_{i-1}) = L(\gamma(X_{i-1} \oplus k_i)$. Two rounds of SMS4 are shown in Figure 1.

The SMS4 S-box.

	-0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-a	-b	-c	-d	-e	-f
0-	d6	90	e9	fe	cc	e1	3d	b7	16	b6	14	c2	28	fb	2c	05
1-	2b	67	9a	76	2a	be	04	c3	aa	44	13	26	49	86	06	99
2-	9c	42	50	f4	91	ef	98	7a	33	54	0b	43	ed	cf	ac	62
3-	e4	b3	1c	a9	c9	08	e8	95	80	df	94	fa	75	8f	3f	a6
4-	47	07	a7	fc	f3	73	17	ba	83	59	3c	19	e6	85	4f	a8
5-	68	6b	81	b2	71	64	da	8b	f8	eb	0f	4b	70	56	9d	35
6-	1e	24	0e	5e	63	58	d1	a2	25	22	7c	3b	01	21	78	87
7-	d4	00	46	57	9f	d3	27	52	4c	36	02	e7	a0	c4	c8	9e
8-	ea	bf	8a	d2	40	c7	38	b5	a3	f7	f2	ce	f9	61	15	a1
9-	e0	ae	5d	a4	9b	34	1a	55	ad	93	32	30	f5	8c	b1	e3
a-	1d	f6	e2	2e	82	66	ca	60	c0	29	23	ab	0d	53	4e	6f
b-	d5	db	37	45	de	fd	8e	2f	03	ff	6a	72	6d	6c	5b	51
c-	8d	1b	af	92	bb	dd	bc	7f	11	d9	5c	41	1f	10	5a	d8
d-	0a	c1	31	88	a5	cd	7b	bd	2d	74	d0	12	b8	e5	b4	b0
e-	89	69	97	4a	0c	96	77	7e	65	b9	f1	09	c5	6e	c6	84
f-	18	f0	7d	ec	3a	dc	4d	20	79	ee	5f	3e	d7	cb	39	48

Appeared in : SAC 2008, LCNS , pp. 0–,

The key schedule. The key schedule is similar to the encryption function. Each subkey k_i is derived as one word from the output of a single round of SMS-like encryption where the "key" for each round i is a constant $g(i)$ (to be defined below). The plaintext for the start of the key generation is the 128-bit user-supplied key $K_{[127\ldots0]}$. The round function for the SMS-like encryption is given by

$$L'(x) = x \oplus (x \lll 13) \oplus (x \lll 23)$$
$$\gamma(x) = (S[x_{31\ldots24}] \,||\, S[x_{23\ldots15}] \,||\, S[x_{15\ldots8}] \,||\, S[x_{7\ldots0}])$$

so only the L-function is changed in comparison with encryption. At the start, the user-supplied key is xor-ed with a constant

$$T = \texttt{0xa3b1bac6 0x56aa3350 0x677d9197 0xb27022dc},$$

and the initialization of the generation of the subkeys[1] is as follows:

$$k_{-3} = K_{[127\ldots96]} \oplus T_{[127\ldots96]}, \quad k_{-2} = K_{[95\ldots64]} \oplus T_{[95\ldots64]},$$
$$k_{-1} = K_{[63\ldots32]} \oplus T_{[63\ldots32]}, \quad k_0 = K_{[31\ldots0]} \oplus T_{[31\ldots0]}.$$

The key k_i for the i^{th} round, for $1 \leq i \leq 32$ is computed as

$$k_i = k_{i-4} \oplus L'(\gamma(k_{i-3} \oplus k_{i-2} \oplus k_{i-1} \oplus g(i)))$$

where each constant $g(i)$ is defined by

$$g(i) = ((28 \times (i-1)) \,||\, (28 \times (i-1)+7) \,||\, (28 \times (i-1)+14) \,||\, (28 \times (i-1)+21)).$$

2.1 RED-SMS4: A small version of SMS4

We confirm some of the work in this paper with experiments, and for these we will need to define a reduced-version of SMS4. This will be a block cipher with a 64-bit key and block size which uses a 4-bit S-box S_r. For experiments we chose the S-box used in PRESENT [2]. We can define a reduced L_r function and a reduced γ_r function as follows:

$$L_r(x) = x \oplus (x \lll 8) \oplus (x \lll 10)$$
$$\gamma_r(x) = (S_r[x_{15\ldots12}] \,||\, S_r[x_{11\ldots8}] \,||\, S_r[x_{7\ldots4}] \,||\, S_r[x_{3\ldots0}]).$$

L_r was built using the rotations that appear in L modulo 16. In this way, the round function f_r used in the i^{th} round of reduced-SMS4 is given by $f_r(X_{i-1}) = L_r(\gamma_r(X_{i-1} \oplus k_i)$. A reduced version of the key schedule requires us to change the linear function L' to L'_r just as we changed L to L_r in the encryption routine, and to revise the per-round constants to $g_r(i) = ((28 \times (i-1)) \,||\, (28 \times (i-1)+7))$.

[1] This is slightly different to other descriptions so as to accommodate the natural numbering of rounds starting with 1.

Appeared in : SAC 2008, LCNS , pp. 0–,

3 Linear cryptanalysis

While linear cryptanalytic methods appeared in [21], the linear cryptanalytic attack and its application to DES was developed by Matsui [12,13]. The basic idea is to find a *linear approximation* to the action of the block cipher. By this we mean a linear equation that includes a bits of the plaintext $P_{r_1}, \ldots, P_{r_a}$, together with b bits of the ciphertext $C_{s_1}, \ldots, C_{s_b}$ and a single bit of key-related information κ. Borrowing the vector inner-product, we will use the notation $\alpha \cdot P$ to denote the sum of plaintext bits $P_{r_1} \oplus \ldots \oplus P_{r_a}$ where $\alpha = \sum_{j=1}^{a} 2^{r_j}$ and α is called a *linear mask*. We will then write a single linear approximation as

$$\alpha \cdot P \oplus \beta \cdot C = \kappa. \tag{1}$$

If κ (the exclusive-or of subkey bits) is fixed, then Equation 1 will be correct with probability $p = \frac{1}{2} + \epsilon$ and we say that the linear approximation has a bias of ϵ. Given a bias of sufficiently large absolute value $|\epsilon|$ and sufficiently many known plaintext/ciphertext pairs, the value of κ can be deduced thereby revealing one bit of key information. Throughout the paper the term "bias" will refer to its absolute value.

It is well-known that we can recover more bits of the key by using Matsui's *Algorithm 2* [12]. Here we use a linear approximation over several inner rounds, say rounds b to c of the r-round cipher, and this approximates one *inner* bit of key information (which is a function of the subkeys $k_b, \ldots, k_c$). Since the inputs to this linear approximation are a function of the plaintext, the ciphertext, and the outer subkeys $k_1, \ldots, k_{b-1}$ and $k_{c+1}, \ldots, k_r$, if we were to test for a bias as part of an exhaustive search over these *outer* key bits, then we would expect a bias to appear for the correct guess. In this way we can recover more key information and derive a more practical attack.

Clearly the basic building block to all these attacks will be the linear approximation, and to build a linear approximation we approximate individual components of the cipher and join these together. We will therefore use the following notation for the linear approximation of a component f, say, where we write $\alpha \xrightarrow{f} \beta$ if $\alpha \cdot X = \beta \cdot f(X)$ with some associated bias ϵ. Approximations to larger components of a block cipher, such as a round, can be written in the same way.

3.1 Linear cryptanalysis and SMS4

To find a linear approximation of SMS4, we first compute the biases of all linear approximations $\alpha \xrightarrow{S} \beta$ to the S-box. Then we consider the evolution of a linear mask through the function L. For this, we define the function

$$L_2(x) = x \oplus (x \ggg 2) \oplus (x \ggg 10) \oplus (x \ggg 18) \oplus (x \ggg 24)$$

and we observe the following. Since for bit-wise rotations $\alpha \cdot (x \lll i) = (\alpha \ggg i) \cdot x$, we have for all 32-bit inputs x, and all linear masks α, that $\alpha \cdot L(x) = L_2(\alpha) \cdot x$.

Appeared in : SAC 2008, LCNS , pp. 0–,

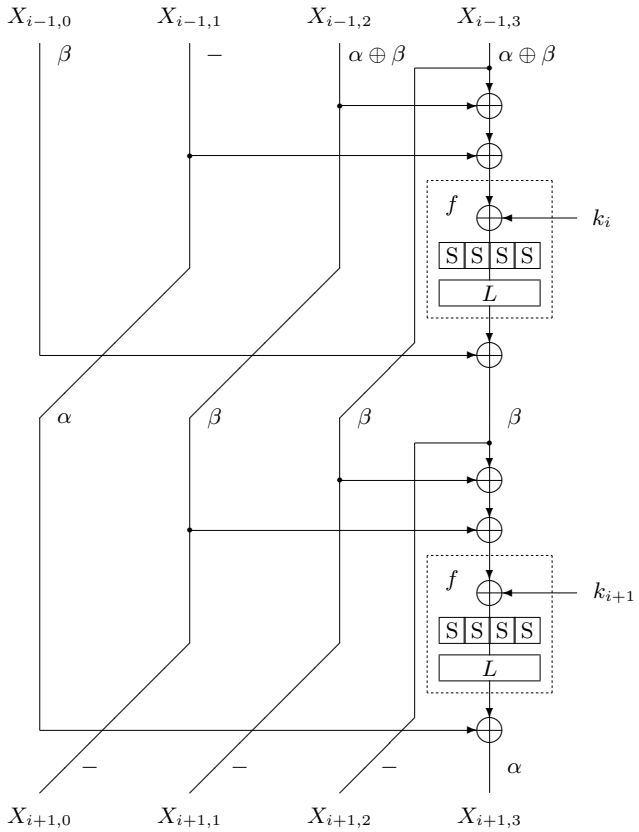

Figure 1. Two rounds of SMS4 along with a two-round linear approximation using masks α and β. The input to round i is $X_{i-1,0} \,||\, X_{i-1,1} \,||\, X_{i-1,2} \,||\, X_{i-1,3}$.

As can be seen from Figure 1, we can identify the potential for two-round linear characteristics of the following form:

$$(\beta, 0, \alpha \oplus \beta, \alpha \oplus \beta) \rightarrow (\alpha, \beta, \beta, \beta) \rightarrow (0, 0, 0, \alpha).$$

Such a linear approximation would require the approximation $\alpha \xrightarrow{f} \beta$ in the first round and $\beta \xrightarrow{f} \alpha$ in the second. Interestingly, by setting $\beta = \alpha$ this reduces to

$$(\alpha, 0, 0, 0) \rightarrow (\alpha, \alpha, \alpha, \alpha) \rightarrow (0, 0, 0, \alpha)$$

and by exploiting the structure of SMS4 in the preceeding three rounds, we derive a five-round iterative linear approximation, of which only the last two rounds are active

$$(0, 0, 0, \alpha) \rightarrow (0, 0, \alpha, 0) \rightarrow (0, \alpha, 0, 0) \rightarrow (\alpha, 0, 0, 0) \rightarrow (\alpha, \alpha, \alpha, \alpha) \rightarrow (0, 0, 0, \alpha).$$

Appeared in : SAC 2008, LCNS , pp. 0–,

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

Table 1. The relevant bitmasks for the iterative linear approximations in this paper.

To identify a bit-mask α that yields an approximation $\alpha \xrightarrow{f} \alpha$ with a good bias, we use the distribution table for linear approximations of the S-box. In this way we can list 24 different $(\alpha, L_2(\alpha))$ pairs, where $L_2(\alpha)$ gives the mask for the output from the S-boxes, and each of these 24 five-round linear approximations holds with a bias of $\frac{7}{32768} \approx 2^{-10.2}$. These are given in Table 1.

3.2 A distinguisher for 18-round SMS4

It is straightforward to see that a classical application of linear cryptanalysis gives us an 18-round distinguisher for SMS4. We can concatenate three of the five-round iterative approximations to give the following 18-round linear approximation with bias ϵ_1:

$$(0,0,0,\alpha) \xrightarrow{5\ rounds} (0,0,0,\alpha) \xrightarrow{5\ rounds} (0,0,0,\alpha)$$
$$\xrightarrow{5\ rounds} (0,0,0,\alpha) \rightarrow (0,0,\alpha,0) \rightarrow (0,\alpha,0,0) \rightarrow (\alpha,0,0,0)$$

To combine linear approximations, and to estimate the resultant bias, it is typical to appeal to the so-called *piling-up lemma* [12]. The suitability of applying the piling-up lemma depends on the algorithms in question; for some, such as DES [15], it gives accurate results while for others, such as RC5 [18], an inter-round dependence means that the piling-up lemma can be misleading [19]. This problem can be particularly acute when we have two consecutive active rounds. However, experimental results below suggest that the piling-up lemma should remain a reasonable tool to use with SMS4. We therefore estimate the resultant bias of the 18-round linear approximation to be $\epsilon_1 = (2^{-10.2})^6 \times 2^5 = 2^{-56.2}$. This means that if we were to use $\epsilon_1^{-2} = 2^{112.4}$ known plaintexts then we would expect our distinguisher to identify non-ideal behaviour in the reduced-round SMS4 and/or to recover a single bit of key information with a success rate of 97.7% [12]. With regards to the work effort, we need to evaluate a single bit

Appeared in : SAC 2008, LCNS , pp. 0–,

and increment a single counter $2^{112.4}$ times. This will be a fraction of the work required to exhaustively search a 128-bit key.

In what follows we will use the 18-round linear approximations of the form described above, of which there are 24 (see Table 1). It will therefore be convenient to refer to a generic approximation from this class as $\mathcal{A}^{18}_{\alpha}$.

Experimental confirmation. To confirm the applicability of the piling-up lemma with the basic linear approximations that we will use, we consider the equivalent linear approximations in RED-SMS4. The bias of the best approximation over a single active round—for which the input and output mask is the same—is 2^{-5}. So over five rounds, of which two are active, the linear approximation $(0,0,0,\alpha) \rightarrow (0,0,0,\alpha)$ with $\alpha = \texttt{0x040c}$ would have a theoretical bias of 2^{-9} . We extend this to give a six-round approximation

$$(\alpha,\beta,\beta,\beta) \xrightarrow{1\ round} (0,0,0,\alpha) \xrightarrow{5\ rounds} (0,0,0,\alpha)$$

with $\beta = \texttt{0x0406}$ and a bias of $2^{-2.7}$ for $\beta \xrightarrow{f_r} \alpha$. The resultant six-round approximation has a theoretical bias of $2^{-10.7}$ and in experiments with 100 keys using the reduced key schedule and 2^{23} known plaintexts, the measured bias ranged between $2^{-10.0}$ and $2^{-12.1}$ with an average of $2^{-10.7}$.

On extending to 19 rounds. Taking $\mathcal{A}^{18}_{\alpha}$ we can prepend a single-round linear approximation of the form $(\alpha,\beta,\beta,\beta) \rightarrow (0,0,0,\alpha)$. Here we can choose β so as to maximise the bias of this extra round. For each of the valid $L_2(\alpha)$ that we identified in Section 3.1, we find that there are 125 possible values to β that give a maximum bias of 2^{-10} over a single round of S-box transformations. This means that there are $125 \times 24 = 3000$ 19-round linear approximations with a bias of $\epsilon_2 = (2^{-10.2})^6 \times 2^{-10} \times 2^6 = 2^{-65.2}$. While the bias means that such approximations aren't immediately useful to us, the large number of such approximations makes them a tempting object for more advanced analysis, see Section 5.1.

4 Advanced techniques

We now use the 18-round approximations $\mathcal{A}^{18}_{\alpha}$ to recover the full 128-bit key. Standard techniques immediately compromise 20-round SMS4, while a novel extension of the work of Collard *et al* [4] extends this to 22 rounds. In the literature notation, this constitutes a 4R-attack for which there are few precedents.

4.1 An attack on 20-round SMS4

The classical approach to using an 18-round distinguisher is to recover key information from the two outer rounds of the cipher. We will use the linear approximations $\mathcal{A}^{18}_{\alpha}$ that have only three active S-boxes in an active round and

Appeared in : SAC 2008, LCNS , pp. 0–,

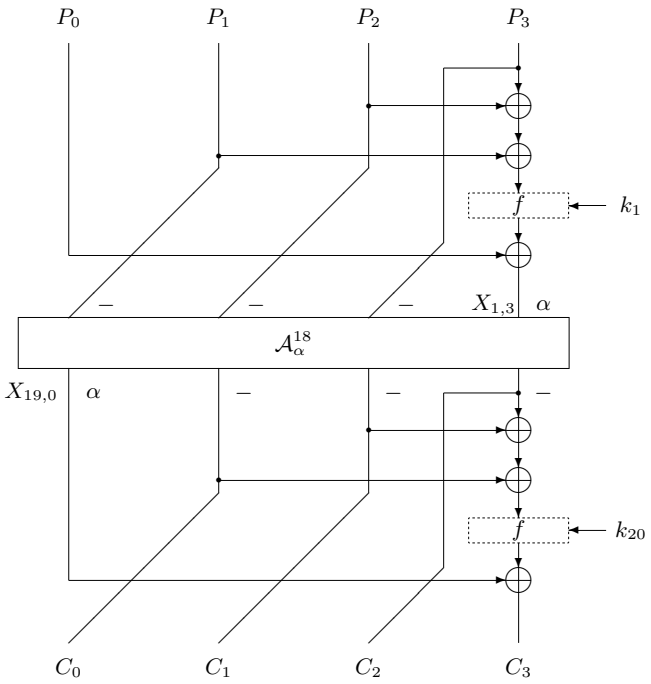

Figure 2. Intermediate values for the 2R attack on 20-round SMS4.

we will need the following definition: Given mask α, denote the *restriction* of a 32-bit word $\mathtt{y}$ by α to be $R_\alpha(\mathtt{y})$ where $R_\alpha(\mathtt{y})$ consists of the deletion of bits corresponding to the inactive byte. For example, given $\alpha = \mathtt{0x0011ffba}$ then $R_\alpha(\mathtt{y}) = \mathtt{y\&0x00ffffff}$. Note that this can be viewed as a 24-bit quantity even when the inactive byte is not in the most significant position.

It is easy to verify the following (see Figure 2). For plaintext $P_0||P_1||P_2||P_3$, the bit value $\alpha \cdot X_{1,3}$ depends solely on $\alpha \cdot P_0$, $R_\alpha(P_1 \oplus P_2 \oplus P_3)$, and $R_\alpha(k_1)$. We can make a similar observation on the ciphertext, namely that the bit value $\alpha \cdot X_{19,0}$ depends solely on $\alpha \cdot C_3$, $R_\alpha(C_0 \oplus C_1 \oplus C_2)$, and $R_\alpha(k_{20})$. In our 2R-attack we will recover the values of $R_\alpha(k_1)$ and $R_\alpha(k_{20})$ giving 48 bits of key information. The rest of the key can be deduced using exhaustive search.

The data-related information that we need to evaluate the approximation is $\alpha \cdot P_0$, $R_\alpha(P_1 \oplus P_2 \oplus P_3)$, $\alpha \cdot C_3$, and $R_\alpha(C_0 \oplus C_1 \oplus C_2)$ and we can consider a plaintext-ciphertext as being in one of 2^{50} possible classes according to the values of these quantities. Note that under the same key guess $R_\alpha(k_1) \,||\, R_\alpha(k_{20})$, two plaintext/ciphertext pairs from the same class yield the same values to $\alpha \cdot X_{1,3}$ and $\alpha \cdot X_{19,0}$. In [4] an efficient 1R-attack is described. We extend this approach

Appeared in : SAC 2008, LCNS , pp. 0–,

to give a 2R-attack recovering information from both outer rounds and adopting an optimisation that means we need only store 2^{48} rather than 2^{50} counters.

1. Take $N = 32\epsilon^{-2} = 2^{117.4}$ plaintext/ciphertext pairs.
2. Initialise a set of counters $A[0] \ldots A[2^{48} - 1]$ to zero.
3. For each plaintext/ciphertext pair, compute $b = \alpha \cdot P_0 \oplus \alpha \cdot C_3$ and increment $A[R_\alpha(P_1 \oplus P_2 \oplus P_3)||R_\alpha(C_0 \oplus C_1 \oplus C_2)]$ if $b = 0$ or decrement it if $b = 1$, *i.e.*
$$A[R_\alpha(P_1 \oplus P_2 \oplus P_3)||R_\alpha(C_0 \oplus C_1 \oplus C_2)] \texttt{ += } (-1)^{(\alpha \cdot P_0 \oplus \alpha \cdot C_3)}.$$
4. For each key guess $k' = R_\alpha(k_1) \,||\, R_\alpha(k_{20})$ keep a counter, and compute the bias generated during the attack as follows:
   (a) Taking each $x = R_\alpha(P_1 \oplus P_2 \oplus P_3)||R_\alpha(C_0 \oplus C_1 \oplus C_2)$ in turn, where $0 \le x \le 2^{48} - 1$, compute the value
   $$c = (-1)^{(\alpha \cdot f(R_\alpha(k_1 \oplus P_1 \oplus P_2 \oplus P_3)) \oplus (\alpha \cdot f(R_\alpha(k_{20} \oplus C_0 \oplus C_1 \oplus C_2))}.$$
   (b) Add $c \times A[R_\alpha(P_1 \oplus P_2 \oplus P_3) \,||\, R_\alpha(C_0 \oplus C_1 \oplus C_2)]$ to the score for key guess k'.
5. After recovering the 48-bit k', perform exhaustive search on the remaining 80 bits of key.

We expect to recover the right value to the 48 bits of the key by identifying the guess which gives the highest score of absolute value; using [20] the correct key should be recovered with a probability of 99.9%

While the work effort for each plaintext/ciphertext pair in step 3 is much less than a round of SMS4, we might estimate the work effort for the first three steps to be equivalent to $2^{117.4} \times \frac{1}{20} \approx 2^{113.1}$ 20-round SMS4 computations. The work effort for finding the right 48 bits of key material in step 4 is $2^{48} \times 2^{48} = 2^{96}$ basic operations and the work to recover the rest of the key. is $2^{128-48} = 2^{80}$ reduced-round SMS encryptions. One point of detail: it is possible (see below) that several keys are identified along with the correct one. However this is not uncommon, and merely extends the search for the remainder of the key.

An optimisation. Even though the work effort for Step 4 is lower than that for data processing, we can adapt techniques introduced in [4]. Consider initialising a $(2^{48} \times 2^{48})$ matrix M, where rows are indexed by $R_\alpha(k_1) \,||\, R_\alpha(k_{20})$ and the columns indexed by $R_\alpha(P_1 \oplus P_2 \oplus P_3) \,||\, R_\alpha(C_0 \oplus C_1 \oplus C_2)$. Then the bias for the i^{th} guess of $R_\alpha(k_1) \,||\, R_\alpha(K_{20})$ is given by $\sum_{j=0}^{2^{48}-1} M_{(i,j)} x_j$ and we can view the counters $A[\cdot]$ as a column vector $\mathbf{x} = A^T$. Following [4], since entry $M_{(i,j)}$ is a function of $i \oplus j$ the entire matrix $M_{(i,j)}$ can be reconstructed from a single row or column, and it is possible to compute the product $M\mathbf{x} = \mathbf{e}$ with only three products between a Discrete Fourier Transform matrix and a vector [4].This means that the complexity of generating a set of final scores for each key, represented by a vector $\mathbf{e}$ is reduced from $O((2^{48})^2)$ to $3 \times O(2^{48} \log_2(2^{48}))$ [4]. The work effort for data analysis can therefore be estimated as $2^{48} \times 3 \times 48 \approx 2^{55.2}$ basic operations.

Appeared in : SAC 2008, LCNS , pp. 0–,

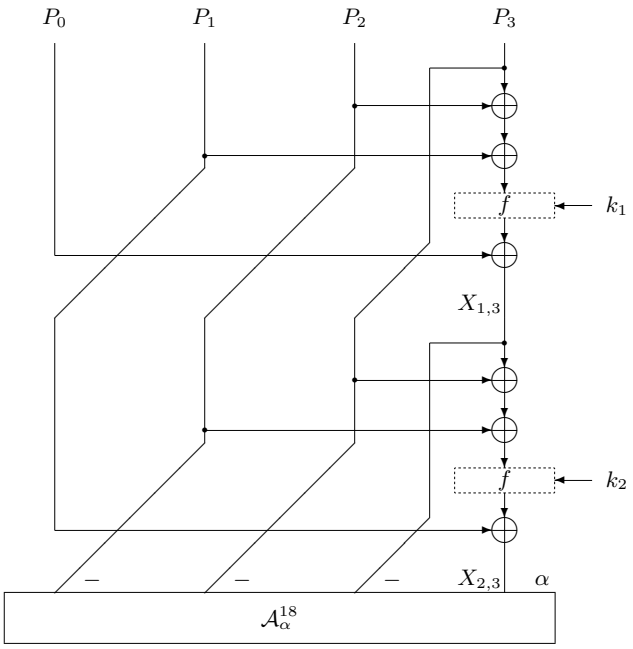

Figure 3. The upper half of the 4R-attack on 22-round SMS4.

Experimental confirmation. To illustrate this more advanced linear attack, we use a 10-round version of RED-SMS4 with the same linear approximation as was used in the experiments of Section 3.2, namely $(\alpha, \beta, \beta, \beta) \rightarrow (\alpha, 0, 0, 0)$ over nine rounds. We will recover information about k_{10}, though for RED-SMS4 the mask α we use has two inactive bytes. Recalling the bias of the approximation is $2^{-10.7}$, we take $8 \times (2^{11})^2 = 2^{25}$ plaintexts. The data is separated according to the restriction $R_\alpha(C_0 \oplus C_1 \oplus C_2)$ and we perform key recovery as outlined in Section 4.1, though adapted to the 1R-scenario. For S_r there is a slight complication with the bit mask α since there are equivalent keys for one of the active nibbles. Experiments and analysis show that the best score applies to four equivalent key values, and so we recover at most six bits of k_{10}. With the plaintext amount we use, we theoretically have a probability of 99.9% to recover the right six bits of key [20]. In 100 experiments the correct set of keys was recovered 99 times.

4.2 An attack on 22-round SMS4

We use $\mathcal{A}_\alpha^{18}$ to make a 4R-attack on 22-round SMS4 (see Figure 3 for the plaintext side of the attack) and we aim to recover k_1, k_{22}, $R_\alpha(k_2)$ and $R_\alpha(k_{21})$. For the data analysis, we will appeal to the optimisation of Collard *et al.* [4] described in Section 4.1.

Appeared in : SAC 2008, LCNS , pp. 0–,

1. We take $N = 64\epsilon^{-2} = 2^{118.4}$ plaintext/ciphertext pairs.
2. View counters $A[0] \ldots A[2^{112} - 1]$ as a column vector $\mathbf{x}$ and set to zero.
3. For each plaintext/ciphertext pair, compute $b = \alpha \cdot P_1 \oplus \alpha \cdot C_2$ and increment $A[P_1 \oplus P_2 \oplus P_3 \,||\, R_\alpha(P_0 \oplus P_2 \oplus P_3) \,||\, R_\alpha(C_0 \oplus C_1 \oplus C_3) \,||\, C_0 \oplus C_1 \oplus C_2]$ if $b = 0$ or decrement it if $b = 1$.
4. Define (conceptually) the $(2^{112} \times 2^{112})$ matrix $M_{(i,j)}$ where rows are indexed by the key guess $k' = k_1 \,||\, R_\alpha(k_2) \,||\, R_\alpha(k_{21}) \,||\, k_{22}$ and columns indexed by $x = P_1 \oplus P_2 \oplus P_3 \,||\, R_\alpha(P_0 \oplus P_2 \oplus P_3) \,||\, R_\alpha(C_0 \oplus C_1 \oplus C_3) \,||\, C_0 \oplus C_1 \oplus C_2$. Recall we need only store the first column of this matrix $M_{(i,j)}$ since all values for subsequent computations can be reconstructed from a single row/column.
   (a) Compute the values in the first column as $(-1)^b$ where
   $$b = \alpha \cdot f(R_\alpha(k_{21} \oplus C_0 \oplus C_1 \oplus C_3) \oplus f(k_{22} \oplus C_0 \oplus C_1 \oplus C_2)) \\ \oplus \alpha \cdot f(R_\alpha(k_2 \oplus P_0 \oplus P_2 \oplus P_3) \oplus f(k_1 \oplus P_1 \oplus P_2 \oplus P_3))$$
   (b) Efficiently compute $M\mathbf{x} = \mathbf{e}$ using [4]. This gives the right result since
   $$\begin{aligned} \alpha \cdot X_{2,3} &= \alpha \cdot f(R_\alpha(k_2) \oplus R_\alpha(P_2 \oplus P_3 \oplus X_{1,3})) \oplus \alpha \cdot P_1 \\ &= \alpha \cdot f(R_\alpha(k_2) \oplus R_\alpha(P_0 \oplus P_2 \oplus P_3) \\ &\quad \oplus f(k_1 \oplus P_1 \oplus P_2 \oplus P_3)) \oplus \alpha \cdot P_1 \end{aligned}$$
   and we have a similar expression for the ciphertext side.
5. Recover the 112-bit k' from $\mathbf{e}$ and search the remaining bits of the key.

The only hypothesis needed to apply [4] to the 22-round attack is that the $(2^{112} \times 2^{112})$ matrix $M_{(i,j)}$ (see optimisation to Section 4.1) should only depend on $i \oplus j$, which is the case for the expression in Step 2. We expect to recover the right value to the 112 bits of the key from the guess with the highest score of absolute value. With $2^{118.4}$ plaintexts, the method of [20] suggests that we are very likely to recover the correct value, see Table 2. The work effort for Steps 1-3 can be estimated as $2^{118.4} \times \frac{1}{22} \approx 2^{113.9}$ 22-round SMS4 computations while the effort in Step 4 is approximately $2^{112} \times 3 \times 112 \times \frac{1}{22} \approx 2^{115.9}$ 22-round SMS4 computations, and this dominates the attack.

5 Ongoing and future research

It is natural to consider some more advanced techniques in trying to attack more rounds of SMS4. In this section we consider the use of multiple linear approximations as well as the use of chosen-plaintexts.

5.1 Multiple linear approximations

Multiple linear approximations were first proposed in [6,7] and they have been the subject of much recent analysis [3,5]. Here we take m different linear approximations, where we use κ_j to denote a single bit of key information,

$$\alpha_j \cdot P \oplus \beta_j \cdot C = \kappa_j.$$

Appeared in : SAC 2008, LCNS , pp. 0–,

r	*texts*	*mem.*	*work steps 1-3*	*work step 4* (w/o [4])	*work step 4* (w. [4])	*work step 5*	*success (%)*
19	$2^{116.4}$	2^{24}	$2^{112.2}$	$2^{43.8}$	2^{26}	2^{104}	99.5
20	$2^{117.4}$	2^{48}	$2^{113.1}$	$2^{91.7}$	$2^{50.9}$	2^{80}	99.9
21	$2^{117.4}$	2^{80}	$2^{113.0}$	$(2^{155.6})$	$2^{83.5}$	2^{48}	84.8
21	$2^{118.4}$	2^{80}	$2^{114.0}$	$(2^{155.6})$	$2^{83.5}$	2^{48}	99.9
22	$2^{117.4}$	2^{112}	$2^{112.9}$	$(2^{219.5})$	$2^{115.9}$	2^{16}	17.7
22	$2^{118.4}$	2^{112}	$2^{113.9}$	$(2^{219.5})$	$2^{115.9}$	2^{16}	99.9

Table 2. The estimated work efforts for a range of linear cryptanalytic attacks on r-round SMS4 for $19 \leq r \leq 22$. Work is estimated in terms of the number of r-round encryptions (for appropriate r) with that exceeding 2^{128} placed in parentheses.

The purpose is to use several approximations to reduce the number of plaintexts when keeping the same probability of sucess. Let ϵ^j denote the theoretical bias of the j^{th} approximation and let $e^j_{k_{\text{outer}}}$ denote the experimental bias of the j^{th} approximation observed when using the guess k_{outer} for the outer key bits[2]. If, with sufficiently many plaintexts, we compute

$$\min_{k_{\text{outer}}} \min_{(\kappa_1,\ldots,\kappa_m)\in\{0,1\}^m} \sum_{j=1}^{m} \left(\epsilon^j - (-1)^{\kappa_j} e^j_{k_{\text{outer}}}\right)^2,$$

then the minimum value will be given by the correct values of k_{outer} and the correct values of the m bits of internal key represented by $(\kappa_1, \ldots, \kappa_m)$.

A straightforward application of this method needs $2^{|k|+m}$ computations. However this can be reduced if we introduce σ^j_k where $\sigma^j_k = 1$ if $sgn(\epsilon^j) = sgn(e^j_k)$ and zero otherwise. Then we observe that, for each j,

$$\min_{\kappa_j\in\{0,1\}} \left(\epsilon^j - (-1)^{\kappa_j} e^j_k\right)^2 = \left(\epsilon^j - (-1)^{\sigma^j_k} e^j_k\right)^2$$

and so we have the equality

$$\begin{aligned}&\min_{k_{\text{outer}}} \min_{(\kappa_1,\ldots,\kappa_m)\in(0,1)^m} \sum_{j=1}^{m} \left(\epsilon^j - (-1)^{\kappa_j} e^j_{k_{\text{outer}}}\right)^2 \\ &= \min_{k_{\text{outer}}} \sum_{j=1}^{m} \left(\epsilon^j - (-1)^{\sigma^j_{k_{\text{outer}}}} e^j_{k_{\text{outer}}}\right)^2.\end{aligned}$$

This requires $m2^{|k_{\text{outer}}|}$ computations, though we only recover the correct value to k_{outer}. However this is usually the most important block of key information to recover.

[2] An equivalent approach considers the *imbalance* which is double the bias [3].

Appeared in : SAC 2008, LCNS , pp. 0–,

Application to SMS4. To gauge the possible limits of linear cryptanalysis, we will optimistically assume that the gain that can be made when using multiple linear approximations is linear in the number of approximations. We will then use the techniques above to combine a set of different linear 19-round approximations and illustrate the basis for a possible attack on 23-round SMS4.

To do this we need a set of linear approximations and we will choose 125 19-round approximations $\mathcal{A}^{19}_{\alpha\beta}$ where these are the extensions of a given, fixed, 18-round distinguisher $\mathcal{A}^{18}_{\alpha}$ by the 125 choices for β. (These approximations were identified in Section 3.2). We denote by ϵ the theoretical bias of $2^{-65.2}$ which is the same for each of the $\mathcal{A}^{19}_{\alpha\beta}$.

1. Take $N = 2^{125.4}$ plaintext/ciphertext pairs.
2. For each β view counters $A[\beta][0], \ldots, A[\beta][2^{112}-1]$ as a column vector $\mathbf{x}^\beta$ and set this to zero.
3. For each β and each plaintext/ciphertext pair, compute $b = \alpha \cdot P_2 \oplus \beta \cdot P_0 \oplus \beta \cdot P_1 \oplus \beta \cdot P_3 \oplus \alpha \cdot C_2$ and increment $A[\beta][P_1 \oplus P_2 \oplus P_3 \,||\, R_\alpha(P_0 \oplus P_2 \oplus P_3) \,||\, R_\alpha(C_0 \oplus C_1 \oplus C_3) \,||\, C_0 \oplus C_1 \oplus C_2]$ if $b = 0$ or decrement it if $b = 1$.
4. Define for each β (conceptually) the $(2^{112} \times 2^{112})$ matrix $M^\beta_{(i,j)}$ where rows are indexed by the outer key guess $k_{\text{outer}} = k_1 \,||\, R_\alpha(k_2) \,||\, R_\alpha(k_{21}) \,||\, k_{22}$ and columns indexed by $x = P_1 \oplus P_2 \oplus P_3 \,||\, R_\alpha(P_0 \oplus P_2 \oplus P_3) \,||\, R_\alpha(C_0 \oplus C_1 \oplus C_3) \,||\, C_0 \oplus C_1 \oplus C_2$. Recall we need only store the first column of this matrix $M^\beta_{(i,j)}$ since all values for subsequent computations can be reconstructed from a single row/column.
5. Compute the values in the first column as $(-1)^b$ where

$$b = \alpha \cdot f(R_\alpha(k_{21} \oplus C_0 \oplus C_1 \oplus C_3) \oplus f(k_{22} \oplus C_0 \oplus C_1 \oplus C_2)) \\ \oplus \beta \cdot f(R_\alpha(k_2 \oplus P_0 \oplus P_2 \oplus P_3) \oplus f(k_1 \oplus P_1 \oplus P_2 \oplus P_3))$$

6. Efficiently compute $M^\beta \mathbf{x}^\beta = \mathbf{e}^\beta$ using [4].
7. For each guess to k_{outer}, compute $\sum_\beta \left(\epsilon - (-1)^{\sigma^\beta_{k_{\text{outer}}}} e^\beta_{k_{\text{outer}}}\right)^2$.
8. Assume that the minimum value is given by the correct guess for the 112-bit k_{outer} and then search the remaining bits of the key.

The work effort for this attack is dominated by Step 3. To derive the maximum number of plaintexts we can use, we observe that the work effort of Step 3 can be expressed as $\frac{125 \times N}{23}$ 23-round SMS4 computations. To give an academic attack, we need this to be less than 2^{128} 23-round SMS4 computations and so we have $N \leq \frac{23 \times 2^{128}}{125} \approx 2^{125.4}$ for a valid attack.

However $2^{125.4}$ corresponds to around $4 \times \frac{(2^{65.2})^2}{125}$, but since we are recovering 112 bits of key information the success rate [20] will be almost negligible. Thus while it is conceivable that 23 rounds could be attacked (academically) we feel that this is somewhat optimistic.

Unfortunately the reduced version of SMS4 used earlier doesn't exhibit different linear approximations with the same bias. Intead we were able to experiment on a different reduced cipher design, but it was too far-removed from SMS4 for us

Appeared in : SAC 2008, LCNS , pp. 0–,

to be able to draw any substantive conclusions. Our experiments demonstrated improvements to the number of plaintexts required in a successful attack, but the probability of success was somewhat less than anticipated by theory. We therefore leave it as an object of future research to provide a sound estimate for the effectiveness of multiple linear approximations on SMS4.

5.2 On using chosen plaintext

Several extensions to linear cryptanalysis consider the use of chosen plaintext. One of these is described by Knudsen and Mathiassen [8]. In early work for this paper we considered using variants of this technique and at first sight it seemed to be well-suited to SMS4. However technical complications meant that it was hard to use these techniques directly with the 18-round distinguisher and we were unable to get any satisfactory advantages. We also considered using differential-linear cryptanalysis [9] but our preliminary conclusion was somewhat negative. We therefore leave it as an open problem to decide whether chosen plaintext can give any real advantage over the typical known plaintext approach.

6 Conclusions

In this paper we have considered the cryptanalysis of the block cipher SMS4. The cipher is both actively deployed and of an elegant and simple design, making it of considerable interest to the cryptanalyst. While much of the preceeding work is concentrated on the differential cryptanalysis of SMS4, by turning to linear cryptanalysis we have demonstrated some simple and effective attacks. These yield results which are superior to all previous claims and which, therefore, give the best current attacks on SMS4.

References

1. E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer Verlag, 1993.
2. 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. In P. Paillier and I. Verbauwhede, editors, *Proceedings of CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450-466. Springer-Verlag, 2007.
3. A. Biryukov, C. De Cannière, and M. Quisquater. On Multiple Linear Approximations. In M. Franklin, editor, *Proceedings of Crypto 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 1–22. Springer-Verlag, 2004.
4. B. Collard, F.-X. Standaert, and J.-J. Quisquater. Improving the Time Complexity of Matsui's Linear Cryptanalysis. In K.-H. Nam and G. Rhee, editors, *Proceedings of ICISC 2007*, volume 4817 of *Lecture Notes in Computer Science*, pages 77–88. Springer-Verlag, 2007.
5. B. Collard, F.-X. Standaert, and J.-J. Quisquater. Experiments on the Multiple Linear Cryptanalysis of Reduced-Round Serpent. In K. Nyberg, editor, *Proceedings of FSE 2008*, Lecture Notes in Computer Science, Springer, *to appear*.

Appeared in : SAC 2008, LCNS , pp. 0–,

6. B.S. Kaliski and M.J.B. Robshaw. Linear Cryptanalysis Using Multiple Approximations. In Y. Desmedt, editor, *Proceedings of Crypto 1994*, volume 839 of *Lecture Notes in Computer Science*, pages 26–39, Springer-Verlag, 1994.
7. B.S. Kaliski and M.J.B. Robshaw. Linear Cryptanalysis and FEAL. In B. Preneel, editor, *Proceedings of FSE 1994*, volume 1008 of *Lecture Notes in Computer Science*, pages 249–264, Springer-Verlag, 1995.
8. L. Knudsen and J. Mathiassen. A Chosen-Plaintext Linear Attack on DES. In B. Schneier, editor, *Proceedings of FSE 2000*, volume 1978 of *Lecture Notes in Computer Science*, pages 262–272, Springer-Verlag, 2001.
9. S.K. Langford and M.E. Hellman. Differential-Linear Cryptanalysis. In Y. Desmedt, editor, *Proceedings of Crypto 1994*, volume 839 of *Lecture Notes in Computer Science*, pages 17–25, Springer-Verlag, 1994.
10. F. Liu, W. Ji, L. Hu, J. Ding, S. Lv, A. Pyshkin, and R.-P. Weinmann. Analysis of the SMS4 Block Cipher. In J. Pieprzyk, H. Ghodosi, and E. Dawson, editors, *Proceedings of ACISP 2007*, volume 4586 of *Lecture Notes in Computer Science*, pages 158–170, Springer-Verlag, 2007.
11. J. Lu. Attacking Reduced-Round Versions of the SMS4 Block Cipher in the Chinese WAPI Standard. In S. Qing, H. Imai, G. Wang, editors, *ICICS 2007* volume 4861 of *Lecture Notes in Computer Science*, pages 306–318, Springer, 2007.
12. M. Matsui. Linear Cryptanalysis Method for DES Cipher. In T. Helleseth, editor, *Proceedings of Eurocrypt '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397, Springer-Verlag, 1994.
13. M. Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In Y. Desmedt, editor, *Proceedings of Crypto 1994*, volume 839 of *Lecture Notes in Computer Science*, pages 1–11, Springer-Verlag, 1994.
14. S. Murphy. The Independence of Linear Approximations in Symmetric Cryptanalysis. *IEEE Transactions on Information Theory*, 52, pages 5510–5518, 2006.
15. National Institute of Standards and Technology. FIPS 46-3: Data Encryption Standard, November 1998. Available from `http://csrc.nist.gov`.
16. National Institute of Standards and Technology. FIPS 197: Advanced Encryption Standard, November 2001. Available from `http://csrc.nist.gov`.
17. K. Nyberg. Linear Approximation of Block Ciphers. In A. de Santis, editor, *Proceedings of Eurocrypt 1994*, volume 950 of *Lecture Notes in Computer Science*, pages 439–444, Springer-Verlag, 1995.
18. R.L. Rivest. The RC5 Encryption Algorithm. In B. Preneel, editor, *Proceedings of FSE 1994*, volume 1008 of *Lecture Notes in Computer Science*, pages 86–96, Springer-Verlag, 1995.
19. A. Selçuk. New Results in Linear Cryptanalysis of RC5. In S. Vaudenay, editor, *Proceedings of FSE 1998*, volume 1372 of *Lecture Notes in Computer Science*, pages 1–16, Springer-Verlag, 1998.
20. A. Selçuk. On Probability of Success in Linear and Differential Cryptanalysis. *Journal of Cryptology*, 21 (1), pages 131–147, January 2008.
21. A. Tardy-Corfdir and H. Gilbert. A Known Plaintext Attack on FEAL-4 and FEAL-6. In J. Feigenbaum, editor, *Proceedings of Crypto 1991*, volume 576 of *Lecture Notes in Computer Science*, pages 172–182, Springer-Verlag, 1992.
22. L. Zhang, W. Zhang, and W. Wu. Cryptanalysis of Reduced-Round SMS4 Block Cipher. In Y. Mi and W. Susilo, editors,*Proceedings of ACISP 2008*, volume 5107 of *Lecture Notes in Computer Science*, pages 216–229, Springer, 2008.

Appeared in : SAC 2008, LCNS , pp. 0–,