Analysis of the SMS4 Block Cipher

Fen Liu[1], Wen Ji[1], Lei Hu[1], Jintai Ding[2],
Shuwang Lv[1], Andrei Pyshkin[3,⋆], and Ralf-Philipp Weinmann[3]

[1] State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences,
Beijing 100049, China
[2] Department of Mathematical Sciences,
University of Cincinnati,
Cincinnati, OH, 45221, USA
[3] Fachbereich Informatik,
Technische Universität Darmstadt,
64289 Darmstadt, Germany

Abstract. SMS4 is a 128-bit block cipher used in the WAPI standard for providing data confidentiality in wireless networks. In this paper we investigate and explain the origin of the S-Box employed by the cipher, show that an embedded cipher similar to BES can be obtained for SMS4 and demonstrate the fragility of the cipher design by giving variants that exhibit 2^{64} weak keys.

We also show attacks on reduced round versions of the cipher. The best practical attack we found is an integral attack that works on 10 rounds out of 32 rounds with a complexity of 2^{18} operations; it can be extended to 13 rounds using round key guesses, resulting in a complexity of 2^{114} operations and a data complexity of 2^{16} chosen pairs.

Keywords: block ciphers, cryptanalysis, UFN, algebraic structure.

1 Introduction

The Wired Authentication and Privacy Infrastructure (WAPI) standard is an alternative to the security mechanisms for wireless networks that are specified in IEEE 802.11i. It has been submitted to the International Standards Organization (ISO) by the Chinese Standards Association (SAC). Although it was subsequently rejected by the ISO in favour of IEEE 802.11i, WAPI still is officially mandated for securing wireless networks within China.

For protecting data packets, the WAPI standard references a 128-bit block cipher called SMS4 which initially was kept secret. In January 2006, the specification of this block cipher however was declassified and published [6]. Other than a differential power attack [11] in a Chinese journal, no analysis of this cipher has appeared in the open literature.

This document sheds light on the design of this block cipher and present a preliminary analysis of its strength against cryptanalytic attacks.

⋆ Supported by a stipend of the Marga und Kurt-Möllgaard-Stiftung.

J. Pieprzyk, H. Ghodosi, and E. Dawson (Eds.): ACISP 2007, LNCS 4586, pp. 158–170, 2007.

In Section 2 we give a description of the SMS4 cipher. In Section 3 we show how the SMS4 S-Box can be derived algebraically and how an embedding of SMS4 similar to the Big Encryption System (BES) can be obtained. Section 4 describes an practical integral attack on a 10-round version of SMS4 that can be extended to a theoretical attack on 13 rounds. Our results in Section 5 demonstrate the fragility of SMS4; we show that modifications of the round constants can lead to a large subspace of weak keys. Finally, in Section 6 we conclude this paper and summarize our findings.

1.1 Notation

In the following, we agree on the conventions used throughout the rest of this paper.

Since all operations of the cipher are defined on either 8-bit, 32-bit or 128-bit quantities, we shall use the following terminology: 8-bit values will simply be called *bytes*, 32-bit values *words* and 128-bit values will be called *blocks*. Word and block values shall be considered to be in big-endian order, i.e. the most-significant bit is in the leftmost position when writing the value as a bitstring.

Let $w \lll r$ denote a cyclic shift of the word w by r positions to the left. Sometimes we will need to write down blocks or words in which certain bytes are unknown. In these cases the symbol $\star$ shall denote bytes with unknown values.

To concatenate multiple byte values into a word and multiple word values into a block, we define a vector of bytes or words to be equivalent to a word respectively block value. To access individual bit ranges of a value w we shall use the notation $w_{[i\ldots j]}$ to extract bits i to j, e.g. for $w \in \mathbb{Z}_{2^{32}}$ the expression $w_{[7\ldots 0]}$ denotes the lowestmost byte of the word value w.

2 Description of the SMS4 Block Cipher

In this section we will give a top-down description of the SMS4 block cipher.

SMS4 is a 32 round unbalanced Feistel network; both the block and the key size are 128 bits. Following the terminology of [10], the cipher is a homogeneous, complete, source-heavy (96:32) UFN with 8 cycles.

Let the internal state be denoted by $\mathcal{S} = (S_1, S_2, S_3, S_4)$ where $S_i \in GF(2)^{32}$. The round keys of the cipher shall be denoted by $K_i \in GF(2)^{32}$.

Define the linear diffusion function λ as

$$\begin{aligned}\lambda : GF(2)^{32} &\to GF(2)^{32} \\ x &\mapsto x \oplus (x \lll 2) \oplus (x \lll 10) \oplus (x \lll 18) \oplus (x \lll 24)\end{aligned}$$

and the brick-layer function γ applying an 8-bit S-Box to the input 4 times in parallel as:

$$\begin{aligned}\gamma : GF(2)^{32} &\to GF(2)^{32} \\ x &\mapsto (\rho(x_{[31\ldots 24]}), \rho(x_{[23\ldots 16]}), \rho(x_{[15\ldots 8]}), \rho(x_{[7\ldots 0]}))\end{aligned}$$

The F-function then simply is the composition of these two functions

$$\begin{aligned} F : GF(2)^{32} \times GF(2)^{32} &\rightarrow GF(2)^{32} \\ (X, K_i) &\rightarrow \lambda(\gamma(X \oplus K_i)) \end{aligned}$$

and the round function R that maps $\mathcal{S}_i$ to $\mathcal{S}_{i+1}$ under the round key K_i as:

$$\begin{aligned} R : GF(2)^{128} \times GF(2)^{32} &\rightarrow GF(2)^{128} \\ (S_1, S_2, S_3, S_4, K_i) &\mapsto (S_2, S_3, S_4, S_1 \oplus F(S_2 \oplus S_2 \oplus S_3, K_i)) \end{aligned}$$

The key schedule. of the cipher operates in a manner similar to the encryption function. In total, 32 round key words k_i are generated from a 128-bit cipher key. For the key schedule a function F' is used that is almost identical to the round function; the only thing changed is the linear transform. Instead of λ, the following mapping λ' is used:

$$\begin{aligned} \lambda' : GF(2)^{32} &\rightarrow GF(2)^{32} \\ x &\mapsto x \oplus (x \lll 13) \oplus (x \lll 23) \end{aligned}$$

In order to obtain the round keys, the cipher key K is first masked with a so-called system parameter

$$T = \texttt{0xA3B1BAC656AA3350677D9197B27022DC}$$

as follows:

$$\begin{aligned} k_{-4} &= K_{[127..96]} \oplus T_{[127..96]} \\ k_{-3} &= K_{[95..64]} \oplus T_{[95..64]} \\ k_{-2} &= K_{[63..32]} \oplus T_{[63..32]} \\ k_{-1} &= K_{[31..0]} \oplus T_{[31..0]} \end{aligned}$$

The reasoning behind the masking of the cipher key is not explained in the design document. The round key of the i-th round is computed as follows:

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

where κ_i are key constants. The key constants κ_i are of the form

$$\kappa_i = ((28 \cdot i), (28 \cdot i + 7), (28 \cdot i + 14), (28 \cdot i + 21))$$

where each component of the above vector is a byte, the operators $\cdot$ and $+$ denote the multiplication respectively addition in $\mathbb{Z}_{256}$.

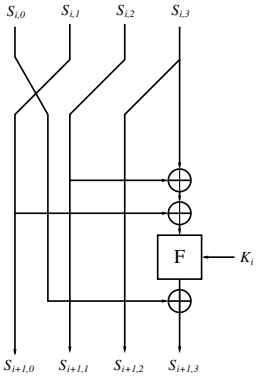

Fig. 1. One round of the SMS4 Unbalanced Feistel Network

3 Algebraic Structure of SMS4

In the SMS4 specification [6], the origin of the S-box is not explained. All the reader is left with is a table with 256 entries. However, we had a hunch that the designers of the cipher had chosen an S-Box design similar to Rijndael; namely that they used an inversion-based mapping. We were confirmed when we looked at the difference distribution table and the linear charateristics of the SMS4 S-Box. These fit our assumption.

3.1 The SMS4 S-Box

We initially assumed the S-Box to be either of the form

$$S(x) = I(x) \cdot A + C, \tag{1}$$

or of the form

$$S(x) = I(x \cdot A + C)$$

where I is the patched inversion over $GF(2^8)$. The matrix $A \in GL(8, 2)$, the vector $C \in GF(2)^8$ and the irreducible polynomial defining the finite field are all undetermined. Experimentally we found that for none of the 30 irreducible polynomials of degree 8, the above expression could be fulfilled for all values of the SMS4 S-Box. However, for a simple permutation of the output bits, we obtained a significant amount of coincident entries between an assumed S-Box of the structure of equation 3.1 and the actual SMS4 S-Box.

The, next idea was to test S-Boxes of the form

$$S(x) = I(x \cdot A_1 + C_1) \cdot A_2 + C_2, \tag{2}$$

with $A_1, A_2 A \in GL(8, 2)$ and $C_1, C_2 \in GF(2)^8$. An exhaustive search for A_1 and C_1 is impractical, because the total number of the 8×8 invertible matrixes is

$$N = \prod_{i=0}^{7} (2^8 - 2^i) \approx 5.348 \times 10^{18} \approx 2^{62}.$$

Because the affine matrix in the algebraic expression of the S-Box in AES is a cyclic matrix, we decided to restrict ourselves to cyclic matrices for A_1 and A_2. Cyclic matrices are determined by their first row. Since there are 255 non-zero binary cyclic 8×8 matrices, we get a total complexity of less than $2^8 \times 2^8 \times 2^8 \times 30 < 2^{29}$, which is practical. In fact, a cyclic matrix with first row $(a_0, a_1, \cdots, a_{n-1})$ is a invertible matrix if and only if the polynomial $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ and $x^n - 1$ are relatively prime. If $n = 8$, this condition is equal to $a_0 + a_1 + \cdots + a_{n-1} \neq 0$. Thus there exist only 2^7 invertible cyclic 8×8 matrices, causing the search complexity to decrease to less than 2^{27}.

Our experiments finally validated the structure of equation 2. We successfully obtained a tuple (A_1, A_2, C_1, C_2) for which all elements of the S-Box all satisfy equation 2. The irreducible polynomial is

$$f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1,$$

the cyclic matrices in the algebraic expression are

$$A_1 = A_2 = \begin{pmatrix} 1&1&1&0&0&1&0&1 \\ 1&1&1&1&0&0&1&0 \\ 0&1&1&1&1&0&0&1 \\ 1&0&1&1&1&1&0&0 \\ 0&1&0&1&1&1&1&0 \\ 0&0&1&0&1&1&1&1 \\ 1&0&0&1&0&1&1&1 \\ 1&1&0&0&1&0&1&1 \end{pmatrix},$$

and the row vectors are

$$C_1 = C_2 = (1, 1, 0, 0, 1, 0, 1, 1).$$

The results presented can also be obtained with less computational effort by using the Affine Equivalence Algorithm for S-Boxes described in [2]. This algorithm in turn is based on the To and Fro algorithm for the isomorphism of polynomials [8].

3.2 Embedding SMS4

Similar to the embedding defined by Murphy and Robshaw for AES–128 [7], we can embed SMS4 into a more elegant and structured cipher ESMS4 in which all operations are performed over the finite field $GF(2^8)$. In this section we will show how this can be done. First note that the description we give is probabilistic, since we do not allow the inversion of the value 0 to occur. The overall number of S-Boxes in the cipher and key schedule is 256, henceforth the probability that an arbitrary plaintext can be encrypted under an arbitrary key without causing a zero inversion can be approximated by $\left(\frac{255}{256}\right)^{256} \approx 1/e \approx 36.7\%$.

First of all, let F denote the field ESMS4 will be defined over:

$$F = GF(2^8) = \frac{GF(2)[x]}{x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1} = GF(2)(\theta)$$

The state space, the key space and the message space of ESMS4 then are F^{128}, the round key space is F^{32}. In accordance with [7] we define a vector conjugate mapping ϕ that maps an element $a \in F$ to an 8-tuple $a \in F^8$

$$\phi(a) = \left(a^{2^0}, a^{2^1}, a^{2^2}, a^{2^3}, a^{2^4}, a^{2^5}, a^{2^6}, a^{2^7}\right)$$

and analogously maps a vector $A \in F^n$ to $A' \in F^{8n}$. The inverse of ϕ, $Im(\phi)$ shall be called extraction mapping. For a $GF(2)$-linear function L operating on a byte $b := (b_8, b_7, b_6, b_5, b_4, b_3, b_2, b_1)$ we obtain a F-linear function $\mathcal{L}$ that performs the equivalent operation on the vector $\phi(b)$ by first computing the coefficients $\beta_1, \ldots, \beta_8$ of the the linearized polynomial

$$\mathcal{L}(b) = \sum_{k=1}^{8} \beta_k a^{2^{k-1}}$$

and then computing the matrix $M_{\mathcal{L}} = (\alpha_{i,j})$ with $\alpha_{i,j} = \beta_{1+((j-i) \bmod 8)}^{2^{i-1}}$. The function $\mathcal{L}$ then is defined as $\mathcal{L} : F^8 \to F^8, v \to M_{\mathcal{L}} \cdot v$. We call $M_{\mathcal{L}}$ the *linearized polynomial matrix form* of L.

The S-Box layer. From Section 3.1 we know that the S-Box of SMS4 can be decomposed into the form $A \circ I \circ A$, with A an affine-linear function over $GF(2)$. Analogously, for ESMS4, the S-Box operation can be performed by $\mathcal{A} \circ \mathcal{I} \circ \mathcal{A}$, with $\mathcal{A}$ being an affine-linear transform over F and $\mathcal{I}$ being the componentwise inversion of elements on a vector $v \in F^8$. The linear part of $\mathcal{A}$ can be expressed by multiplication of the linearized polynomial matrix form $M_{\mathcal{A}} \in F^{8\times 8}$ of the linear part of A, whilst the constant can simply be embedded using ϕ. We define $\widetilde{C} = (\phi(C_1), \phi(C_1), \phi(C_1), \phi(C_1))$ and $\widetilde{A} = \mathrm{Diag}_4(M_{\mathcal{A}})$.

The linear transform $\boldsymbol{\lambda}$. Let $P \in GF(2)^{32\times 32}$ be the permutation matrix such that for $v \in GF(2)^{32}$, the product $P \cdot v$ corresponds to a cyclic shift of elements of v by one position to the left. This matrix can be decomposed into the following form

$$P = \begin{pmatrix} M_1 & 0 & 0 & M_2 \\ M_2 & M_1 & 0 & 0 \\ 0 & M_2 & M_1 & 0 \\ 0 & 0 & M_2 & M_1 \end{pmatrix}, \quad M_1, M_2 \in GF(2)^{8\times 8}$$

By computing the linearized polynomial matrix forms for M_1, M_2

$$\widetilde{M_1} = \mathcal{L}(M_1), \quad \widetilde{M_2} = \mathcal{L}(M_2)$$

we obtain the following matrix that performs the equivalent action on a 32-tuple of elements representing 4 bytes of the state:

$$P = \begin{pmatrix} \widetilde{M_1} & 0 & 0 & \widetilde{M_2} \\ \widetilde{M_2} & \widetilde{M_1} & 0 & 0 \\ 0 & \widetilde{M_2} & \widetilde{M_1} & 0 \\ 0 & 0 & \widetilde{M_2} & \widetilde{M_1} \end{pmatrix}, \quad \widetilde{M_1}, \widetilde{M_2} \in F^{8\times 8}$$

Then the transformation λ is equivalent to the multiplication from the left with the matrix

$$\Lambda_1 = P^0 + P^2 + P^{10} + P^{18} + P^{24}$$

whilst for λ' the corresponding matrix is

$$\Lambda_2 = P^0 + P^{13} + P^{24}.$$

The round function. The F-function function of the cipher ESMS4 can be expressed as:

$$\begin{aligned} \widetilde{F} : F^{32} \times F^{32} &\to F^{32}, \\ (\widetilde{X}, \widetilde{K}) &\mapsto \Lambda_1 \cdot \left(\widetilde{A} \cdot \mathcal{I} \left(\widetilde{A} \cdot \left(\widetilde{X} + \widetilde{K} \right) + \widetilde{C} \right) + \widetilde{C} \right) \end{aligned}$$

The key schedule. The key generation function of ESMS4 is defined in the same way as the F-function except for replacing Λ_1 by Λ_2.

The existence of the embedding stems from the fact that SMS4 uses only $GF(2)$-linear operations and an inversion over $GF(2^8)$. Since the number of S-Boxes per cipher round is only a quarter of that of BES–128, we expect ESMS4 to be more amenable to experimenting with algebraic attacks without resorting to scaling down the field or block size.

4 A Reduced-Round Attack Using Integrals

Integral cryptanalysis is a powerful cryptanalytic method that was first used to break a reduced version of SQUARE [3], a predecessor of Rijndael. In following we will use the notation of [5]. We will use $[A_1, A_2, A_3, A_4]$ to denote a block and (a_1, a_2, a_3, a_4) to denote a word.

Our attack is based on the following difference pairs for the round function of SMS4:

$$\begin{aligned} [\Delta, 0, 0, 0] &\to [0, 0, 0, \Delta] & [0, 0, \Delta, \Delta] &\to [0, \Delta, \Delta, 0] \\ [0, \Delta, \Delta, 0] &\to [\Delta, \Delta, 0, 0] & [0, \Delta, 0, \Delta] &\to [\Delta, 0, \Delta, 0] \end{aligned}$$

All these difference pairs are of probability one.

Table 1. Propagation of the 8 round integral

round no. (r)	$S_{r,1}$	$S_{r,2}$	$S_{r,3}$	$S_{r,4}$
0	(C,C,C,A)	(C,C,C,A)	(C,C,C,A)	(C,C,C,C)
1	(C,C,C,A)	(C,C,C,A)	(C,C,C,C)	(C,C,C,A)
2	(C,C,C,A)	(C,C,C,C)	(C,C,C,A)	(C,C,C,A)
3	(C,C,C,C)	(C,C,C,A)	(C,C,C,A)	(C,C,C,A)
4	(C,C,C,A)	(C,C,C,A)	(C,C,C,A)	(A,A,A,A)
5	(C,C,C,A)	(C,C,C,A)	(A,A,A,A)	(S,S,S,S)
6			(S,S,S,S)	($\star$,$\star$,$\star$,$\star$)
7		(S,S,S,S)	($\star$,$\star$,$\star$,$\star$)	
8	(S,S,S,S)	($\star$,$\star$,$\star$,$\star$)		

Let $P = [P_1, P_2, P_3, P_4]$ be a plaintext. Then the following collection of 256 plaintexts will allow us to attack the 9th round key of SMS4:

$$[P_1 \oplus \delta,\ P_2 \oplus \delta,\ P_3 \oplus \delta,\ P_4],$$

where δ ranges from 0 to 255.

A trace of this integral through the cipher is depicted in Table 1. Each letter C denotes a distinct constant byte value whilst the letter A ranges over all possible byte values. In our case, the letter S means that the sum of all bytes after the γ function is zero. This integral will allow us to determine four key bytes of the last round key.

Moreover, since

$$\gamma(S_{8,2} \oplus S_{8,3} \oplus S_{8,4} \oplus K_i) = \lambda^{-1}(S_{8,1} \oplus S_{9,4}),$$

each key byte can be found independently.

Following the ideas of [4], this attack can be extended by an additional round at the beginning using the following integral:

$$\Delta\ (C, C, C, A)\ (C, C, C, A)\ (C, C, C, A)$$

where $\Delta = \lambda(0, 0, 0, \tilde{A}) \oplus (C, C, C, C)$; with $\tilde{A}$ independently ranging over all byte values. Using a structure of 2^{16} plaintexts allows us to parallelly determine all bytes of the the 10th round key. We have implemented and experimentally verified this attack.

The attack can be extended without increasing the data complexity by guessing additional round keys. A theoretical attack on 13 rounds is thus possible with a complexity of about 2^{114} cipher operations. Generic attacks on Feistel networks with the structure of SMS4 (96:32 UFN) work on a significantly smaller number of rounds, namely up to 7 rounds [9,10].

5 Weak Keys for Modified Round Key Constants

In this section we show that for slightly modified round key constants in the key schedule, the cipher will exhibit a class of 2^{64} weak keys. For all of these keys, the

cipher exhibits an invariant property over an arbitrary number of rounds. This invariance can be used to effectively distinguish the encryption function from a random permutation. Once the use of a weak key is detected, the key search space for an attacker of course shrinks from 2^{128} to 2^{64}. The property shows an unexpected fragility of the cipher design and in our opinion casts serious doubt on its strength.

Definition 1. *Let $a \in GF(2)^{2n}$. If $a = b||b$ for an element $b \in GF(2)^n$, then we say that the element a has a $1/2$-repetition property; alternatively a may be called $1/2$-repeated.*

Theorem 1. *Let $(s_1, \ldots, s_k) \in \mathbb{Z}^k$ be a vector of shift offsets. Any $2n$-bit function $g : GF(2)^{2n} \to GF(2)^{2n}$ of the form*

$$x \mapsto \bigoplus_{i=1}^{k} (x \lll s_i)$$

preserves the $1/2$-repetition property.

Proof. Obviously the invariance condition is preserved under addition if it holds for all elements of the sum. By induction the invariance condition for n-bit cyclic shifts can be derived for 1-bit shits. □

Modifying all round key constants κ_i to be $1/2$-repeated, we obtain 2^{64} cipher keys for which all round keys possess the $1/2$-repetition property; note that due to the masking of the cipher key with the system parameter in the key generation the 2^{64} actual cipher keys are not $1/2$-repeated though. Both the round key function and the round function preserve the invariance for these keys. From this follows that for plaintexs in which each word is $1/2$-repeated, we obtain ciphertexts that also are $1/2$-repeated. Henceforth, these cipher variants are insecure.

6 Conclusions

We have given a detailed analysis of SMS4. Its design seems to be clearly influenced by Rijndael, although the UFN structure makes for a much simpler implementation. We decomposed the S-Box into two affine linear transforms and an inversion and have given an embedding to the cipher similar to BES. An practical attack on 10 rounds of SMS4 has been demonstrated and the fragility of the key schedule has been exposed. We think that our results are only a first step in the cryptanalysis of SMS4 and that further improvements can be made. Especially the point of algebraic cryptanalysis – for which this cipher is an excellent target – has not been addressed in this paper. This will be discussed in a future paper.

References

1. Barkan, E., Biham, E.: In How Many Ways Can You Write Rijndael? In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 160–175. Springer, Heidelberg (2002)
2. Biryukov, A., De Cannière, C., Braeken, A., Preneel, B.: A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. In: Biham, E. (ed.) Advances in Cryptology – EUROCRPYT 2003. LNCS, vol. 2656, pp. 33–50. Springer, Heidelberg (2003)
3. Daemen, J., Knudsen, L.R., Rijmen, V.: The Block Cipher Square. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997)
4. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.: Improved Cryptanalysis of Rijndael. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 213–230. Springer, Heidelberg (2000)
5. Knudsen, L.R., Wagner, D.: Integral Cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
6. Beijing Data Security Technology Co. Ltd. Specification of SMS4 (in Chinese) (2006) `http://www.oscca.gov.cn/UpFile/,21016423197990.pdf`
7. Murphy, S., Robshaw, M.J.B.: Essential Algebraic Structure within the AES. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 1–16. Springer, Heidelberg (2002)
8. Patarin, J., Goubin, L., Courtois, N.: Improved algorithms for isomorphisms of polynomials. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 184–200. Springer, Heidelberg (1998)
9. Patarin, J., Nachef, V., Berbain, C.: Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 396–411. Springer, Heidelberg (2006)
10. Schneier, B., Kelsey, J.: Unbalanced Feistel Networks and Block Cipher Design. In: Gollmann, D. (ed.) Fast Software Encryption. LNCS, vol. 1039, pp. 121–144. Springer, Heidelberg (1996)
11. Zhang, L., Wu, W.: Difference Fault Attack on the SMS4 Encryption Algorithm (in Chinese). Chinese Journal of Computers 29(9) (2006)

Appendix A: The SMS4 S-Box

Below you find the entries of the SMS4 S-Box in hexadecimal notation. For example, for an input of `0xef` the corresponding output can be read off in the row labelled with the value `e` and the column labelled with `f`: `0x84`.

	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

Appendix B: Equivalent Forms of the S-Box

Just as for the Rijndael S-Box [1], different equivalent representations of the SMS4 S-Box can be obtained. The S-Box constructed by equation 2 in Section 3.1 is a composition of two affine transformations and a mapping I in the vector space. I is a mapping in the vector space obtained from an inversion mapping in $GF(2^8)$, it is related to the chosen basis of the finite field. The basis defining I in equation 2 is a polynomial basis $\{\beta^7, \cdots, \beta, 1\}$ (β is a root of the polynomial), which is defined by the irreducible polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$.

Below we study the equivalent forms of algebraic expression of the S-Box, namely we find other algebraic expressions when the inversion mapping of the finite field is represented in different bases. We do not limit ourselves to polynomial bases, we consider general bases of finite fields.

If $\{\alpha_{n-1}, \cdots, \alpha_1, \alpha_0\}$ and $\{\beta_{n-1}, \cdots, \beta_1, \beta_0\}$ are two bases of $GF(2^n)$ over $GF(2)$, there must be a $n \times n$ invertible matrix M that satisfies the equation below

$$\begin{pmatrix} \alpha_{n-1} \\ \vdots \\ \alpha_0 \end{pmatrix} = M \begin{pmatrix} \beta_{n-1} \\ \vdots \\ \beta_0 \end{pmatrix}.$$

M is a transformation matrix from the basis $\{\beta_{n-1}, \cdots, \beta_1, \beta_0\}$ to the basis $\{\alpha_{n-1}, \cdots, \alpha_1, \alpha_0\}$.

Lemma 1. *Let $I_1, I_2 : GF(2)^n \to GF(2)^n$ be mappings corresponding to I under the basis $\{\alpha_{n-1}, \cdots, \alpha_1, \alpha_0\}$ and $\{\beta_{n-1}, \cdots, \beta_1, \beta_0\}$ respectively. Then*

$$I_1(x) = I_2(x \cdot M) \cdot M^{-1}$$

Proof. For any $x \in GF(2^n)$, if the denotation of x under two bases are

$$x = (x_{n-1}, \cdots, x_0) \begin{pmatrix} \alpha_{n-1} \\ \vdots \\ \alpha_0 \end{pmatrix} = (y_{n-1}, \cdots, y_0) \begin{pmatrix} \beta_{n-1} \\ \vdots \\ \beta_0 \end{pmatrix},$$

then

$$(x_{n-1}, \cdots, x_0) \cdot M = (y_{n-1}, \cdots, y_0). \tag{3}$$

While

$$I_1(x_{n-1}, \cdots, x_0) \begin{pmatrix} \alpha_{n-1} \\ \vdots \\ \alpha_0 \end{pmatrix} = I(x) = I_2(y_{n-1}, \cdots, y_0) \begin{pmatrix} \beta_{n-1} \\ \vdots \\ \beta_0 \end{pmatrix},$$

namely that

$$I_1(x_{n-1}, \cdots, x_0) \cdot M \begin{pmatrix} \beta_{n-1} \\ \vdots \\ \beta_0 \end{pmatrix} = I_2(y_{n-1}, \cdots, y_0) \begin{pmatrix} \beta_{n-1} \\ \vdots \\ \beta_0 \end{pmatrix},$$

so

$$I_1(x_{n-1}, \cdots, x_0) \cdot M = I_2(y_{n-1}, \cdots, y_0).$$

Substituting equation 3 into the formula above, we obtain

$$I_1(x_{n-1}, \cdots, x_0) \cdot M = I_2((x_{n-1}, \cdots, x_0) \cdot M),$$

namely for any $x \in GF(2)^n$,

$$I_1(x) = I_2(x \cdot M) \cdot M^{-1}$$

Corollary 1. *Select* $\{\beta_7, \cdots, \beta_1, \beta_0\}$ *as the polynomial basis defined by the irreducible polynomial* $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$. *Let* $\{\alpha_7, \cdots, \alpha_1, \alpha_0\}$ *be another polynomial basis of* $GF(2^8)$ *and* M *be the transformation matrix from* $\{\beta_7, \cdots, \beta_1, \beta_0\}$ *to* $\{\alpha_7, \cdots, \alpha_1, \alpha_0\}$. *Then under the basis* $\{\alpha_7, \cdots, \alpha_1, \alpha_0\}$, *the algebraic expression of the SMS4 S-Box is*

$$S(x) = I_1(xA_1M + C_1M)M^{-1}A_2 + C_2. \tag{4}$$

For convenience, A_1, A_2 of the equation 2 are called generator matrices of the S-Box. According to Corollary 1, under the basis $\{\alpha_{n-1}, \cdots, \alpha_0\}$ the generator matrices of the S-Box are A_1M and $M^{-1}A_2$.

There are 30 irreducible polynomials of degree 8 over $GF(2)$. Every irreducible polynomial can define 8 different bases. Therefore there are $30 \times 8 = 240$ algebraic expressions of the S-Box with different generator matrices. If we do not limit ourselves to polynomial bases, the generator matrix A_1M in the algebraic expression of the S-Box can be any invertible matrix (correspondingly, $M^{-1}A_2$ is another matrix).

Next we will prove that if we limit ourselves to cyclic matrices for A_1, A_2 under a polynomial basis, the basis must be the one mentioned in the previous section. In this sense the algebraic expression presented in 3.1 is the simplemost form that can be obtained.

Proposition 1. *If restrict A_1, A_2 to be cyclic matrices, the algebraic expression of the S-Box (A_1, A_2, C_1, C_2) presented in Section 3.1 is uniquely defined.*

Proof. According to Corollary 1, for the other tuple

$$S(x) = I_1(x \cdot A_1^T \cdot M + C_1 \cdot M) \cdot M^{-1} \cdot A_2^T + C_2. \tag{5}$$

holds. Assume that $(A_1^T \cdot M)$ and $(M^{-1} \cdot A_2^T)$ are cyclic matrices, while A_1, A_2 are cyclic matrices as well. Then M^T and M must also be cyclic matrixes, namely we get

$$\begin{pmatrix} \alpha^{n-1} \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \\ c_7 & c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \\ c_6 & c_7 & c_0 & c_1 & c_2 & c_3 & c_4 & c_5 \\ c_5 & c_6 & c_7 & c_0 & c_1 & c_2 & c_3 & c_4 \\ c_4 & c_5 & c_6 & c_7 & c_0 & c_1 & c_2 & c_3 \\ c_3 & c_4 & c_5 & c_6 & c_7 & c_0 & c_1 & c_2 \\ c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_0 & c_1 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_0 \end{pmatrix} \begin{pmatrix} \beta^{n-1} \\ \vdots \\ 1 \end{pmatrix}$$

We then can get a system of linear equations,

$$\begin{cases} 1 = c_0 + c_1\beta + \cdots + c_7\beta^7 \\ \alpha = c_0\beta + \cdots + c_6\beta^7 + c_7 \\ \vdots \\ \alpha^7 = c_0\beta^7 + c_1 + \cdots + c_6\beta^5 + c_7\beta^6 \end{cases}$$

which can be transformed into:

$$\begin{cases} \alpha - \beta = c_7(1 - \beta^8) \\ \alpha(\alpha - \beta) = c_6(1 - \beta^8) \\ \vdots \\ \alpha^6(\alpha - \beta) = c_1(1 - \beta^8) \end{cases}$$

From this follows that

$$\alpha = \frac{c_6}{c_7} = \frac{c_5}{c_6} = \frac{c_4}{c_5} = \frac{c_3}{c_4} = \frac{c_2}{c_3} = \frac{c_1}{c_2}.$$

Since we know that $(\alpha^7, \cdots, \alpha, 1)^T$ is a polynomial basis, it is impossible for α to satisfy the above form. Hence our initial assumption is wrong. From this follows that for generator matrices limited to cyclic matrices, the generator tuple of the SMS4 S-Box is unique.