OPEN ACCESS
ISSN: 2249-6645

International
Journal
Of Modern Engineering Research (IJMER)

Design and Implementation of SMS4 Cipher Based on Twisted BDD S-Box Architecture

G.Archana[1], K.Praveena[2]

*(Asst.Prof, ECE Dept, CMREC, INDIA) Email: aarchana9@gmail.com
** (Asst.Prof, ECE Dept ECE,CMREC, INDIA) Email: praveenakaitha@gmail.com

ABSTRACT:- SMS4 is a 128-bit block cipher used in the WAPI standard for protecting data packets in WLAN. In this paper, various S-box circuit architectures were evaluated firstly and the twisted BDD with m=4 was proved as the fastest one. A fast SMS4 cipher VLSI implementation was completed based on the twisted BDD S-box architecture, and achieved over 200MHz and 100MHz maximal frequency on SMIC 0.18μ m and Chartered 0.35μ m CMOS technology respectively

Keywords:- *SMS4 cipher; S-box; twisted BDD architecture; VLSI design, WAPI*

I. INTRODUCTION

In 2006, the Office of State Commercial Cipher Administration of China (OSCCA) released the specification of the SMS4 block cipher [1], which was employed in the Wide Authentication and Privacy Infrastructure (WAPI) standard to provide the data confidentiality in wireless networks.

To date, several studies have been performed on the SMS4 cipher, such as differential power analysis [2], differential fault analysis [3][4], the algebraic structure [5], and hardware implementations [6]. However, no research has been reported on speed evaluation and optimization of the SMS4 cipher circuit design.

In this paper, we evaluated various hardware architectures of the S-box and completed a fast SMS4 VLSI design with the twisted binary decision diagram (BDD) S-box architecture presented in [7]. The simulation results indicate that, our design achieves a 200MHz clock frequency on SMIC 0.18μm technology, and 103MHz on Chartered 0.35μm technology.

The rest of this paper is organized as follows. Section II describes the SMS4 block cipher. In section III, some SMS4 S-box circuit architectures are introduced briefly and our evaluation results are presented. A fast full SMS4 VLSI implementation and its simulation results are described in section IV. Finally, conclusions are reported in section V.

II. SMS4 BLOCK CIPHER

SMS4 is a 32-round iterative algorithm, and both the data block and the key size are fixed to 128 bits [1]. The encryption flow of the SMS4 cipher is showed in Fig. 1.

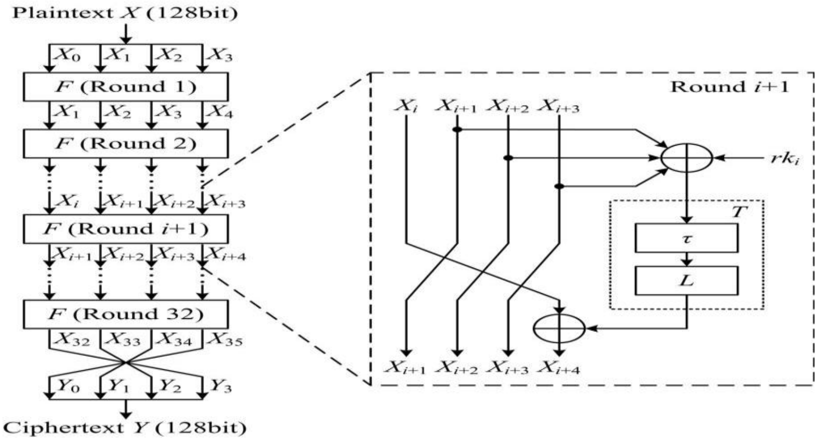


Figure 1. SMS4 cipher encryption process.

A. Encryption Algorithm

Let $X = (X_0, X_1, X_2, X_3)$ €$(GF(2^{32}))^4$ be the plaintext and $Y = (Y_0, Y_1, Y_2, Y_3)$ € $(GF(2^{32}))^4$ be the ciphertext. Let denoted by rk_i €$GF(2^{32})$ the round keys and by $(X_i, X_{i+1}, X_{i+2}, X_{i+3})$ the $(i+1)$-th round inputs, $i=\{0,1,...,31\}$. Then the SMS4 scheme can be written as

$$X_{i\ 4} = F (X_i , X_{i1} , X_{i\ 2} , X_{i\ 3} , rk_i) \quad \textbf{(1)}$$

$$= X_i \oplus T (X_{i\ 1} \oplus X_{i\ 2} \oplus X_{i\ 3} \oplus rk_i)$$

and

$$(Y_0 ,Y_1,Y_2 ,Y_3) = (X_{35} , X_{34} , X_{33} , X_{32}) \quad \textbf{(2)}$$

where $i \in \{0,1,...,31\}$, F is the round function and T is the composite transformation.

The transformation T: $GF(2^{32}) \rightarrow GF(2^{32})$ is composed of the nonlinear transformation τ and the linear transformation

L:

$$T (.) = L(\tau (.)) \quad \textbf{(3)}$$

The transformation τ includes four 8-bit nonlinear S-boxes in parallel. Let denoted by

$$A = (a_0,a_1,a_2,a_3)\ €(GF(2^8))^4$$

The input of τ and by $B = (b_0,b_1,b_2,b_3)$ € $(GF(2^8))^4$ the output. Then τ can be defined as $B=(b_0 ,b_1 ,b_2 ,b_3) = \tau (A)= (Sbox(a_0),\ Sbox(a_1), Sbox(a_2), Sbox(a_3))$ where $Sbox(.)$ is the S-box byte substitution which will be described in detail later. The output of τ, B, is also the input of the linear transformation L. Let denoted by

$$C€GF(2^{32}) \quad \textbf{(4)}$$

the output of L. Then L can be defined as

$$C = L(B) = B \oplus (B<<< 2) \oplus (B<<< 10) \oplus (B <<< 18) \oplus (B <<< 24) \quad \textbf{(5)}$$

where $<<< i$ denotes a 32-bit cyclic left shift by i positions. SMS4 is asymmetric cipher, in which both sender and receiver use a single key for encryption and decryption. The decryption procedure of SMS4 can be done in the same way as the encryption procedure by reversing the order of the round keys.

B. Key Schedule

The key schedule process of SMS4 cipher has the same structur as that in the encryption process except for L function. Let $MK = (MK_0,MK_1,MK_2,MK_3) \oplus (GF(2^{32}))^4$ denote the cipher key rk_i €$GF32\ (2^{32})$, $i\{€0,1,...,31\}$ denote the round K_i €$GF(2)$, $i€\{0,1,...,35\}$. Then key schedule algorithm is defined as

$$(K_0,K_1,K_2,K_3)= (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)\ \textbf{(6)}$$

$$\text{and } rk_i=K_{i+4}=K_i \oplus T'(K_i \oplus K_{i\ 2} \oplus K_{i\ 3} \oplus CK_i)\ \textbf{(7)}$$

where FK_i, $i=\{0,1,2,3\}$ are system parameters, CK_i, $i=\{0,1,2,3\}$ are key constants, and T' is a transformation similar to T in the encryption process. The only difference between T and T' is the linear transformation. Instead of L, the following transformation L *is used in*

$$T'\ L'(B) = B \oplus (B <<< 13) \oplus (B<<< 23)\ \textbf{(8)}$$

The system parameters FK_i are defined in hexadecimal as

$$FK_0\text{=0xA3B1BAC6}, FK_1 = \text{0x56AA3350}, FK_2\text{=0x677D9197}, FK_3 = \text{0xB27022DC}\ \textbf{(9)}$$

The key constants $CK_i = (ck_{i,0}, ck_{i,1}, ck_{i,2}, ck_{i,3})$ € $(GF(2^8))^4$ can be computed as follows:

$$ck_{i,\ j} = (4\times i + j) \times 7(\text{mod } 256)\ \textbf{(10)}$$

where $i=\{0,1,...,31\}$, and $j=\{0,1,2,3\}$.

C. S-box

The S-BOX lookup table of the SMS4 cipher is shown as Table I [1], and the algebraic structure of the S-box can be $Sbox(a) = I (a + \mathbf{A_1}\ C_1) + \mathbf{A_2}\ C_2$ (11) where $I(.)$ is the patched inversion over $GF(2^8)$, the matrices $\mathbf{A_1}$, $\mathbf{A_2}$ €$GL(8,2)$, and the vectors C_1, $C_2 = GF(2)^8$. The cyclic matrices and the row vectors in (11) are as follows

TABLE I. SMS4 S-box LookupTable

	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

$$A1=A2=\begin{array}{cccccccc} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{array} \text{----}\mathbf{(12)}$$

$$C_1 = C_2 = (1,1,0,0,1,0,1,1) \quad \mathbf{(13)}$$

$$f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1 \quad \mathbf{(14)}$$

A. Approaches

Because the SMS4 cipher was released not long ago, few studies have been reported on the S-box circuit architectures. But there are several approaches on the AES S-box circuit. design [7][8], which is very similar to the SMS4 S-box. In the AES S-box implementations, the most intuitive approach is to use the lookup table method, where the S-box circuit is synthesized from the complete S-box mapping table directly using EDA tools. The S-box circuit can be also obtained from its truth table using some logic architectures, such as sum of products (SOP), a BDD and a twisted In addition; compact S-box circuits can be designed based on BDD. In addition, compact S-box circuits can be designed based on mathematical operations over composite fields. In the various S-box circuit architectures, the twisted BDD was reported as the fastest one [7]. In this method, the m levels on the output side in each BDD was replaced by a 2m:1 selector which was comprise of a select-signal decoder and a data selection part to reduce the delay, as shown in Fig. 2. With different m value, the delay of each BDD is different. When m=0, there is no selector replacement described above.

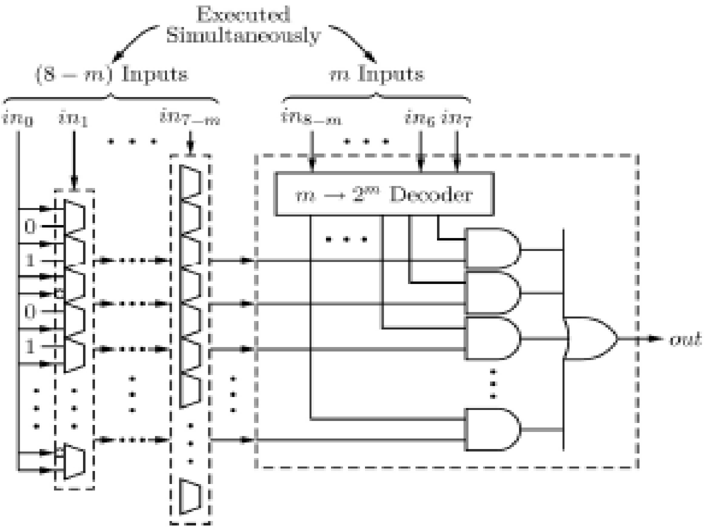


Figure 2. BDD structure in the twisted BDD architecture.

B. Evaluation Results

We completed various S-box circuit architecture designs including coding, logic synthesis and physical design with the same constraint on SMIC 0.18μm and Chartered 0.35μm CMOS technology respectively. The BDDs were constructed using the CUDD package [9].

The area and delay of the S-box designs are shown in Table II and Table III. From the implementation results, we can find that the twisted BDD with *m*=4 is the fastest architecture and it is more than 26% and 30% faster than the directly synthesized lookup table method on SMIC 0.18μm and Chartered 0.35μm technology, respectively. Although the absolute values of the delay and area also depend on the technology, EDA tools and synthesis constraints, the comparisons of the performances between the various architectures are almost the same.

III. FAST SMS4 VLSI IMPLEMENTATION

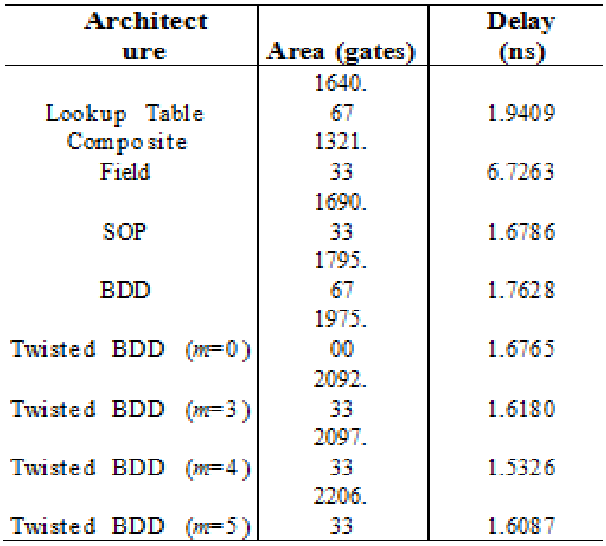
According to the evaluation results in section III, we selected the twisted BDD with *m*=4 as the S-box architecture in our SMS4 VLSI design to obtain a higher speed.

A. BDDs Construction

We calculated out the sizes of the BDDs with all possible input orders using the CUDD package firstly. The size ranges of the BDDs are shown in Table IV. From the results, we can find that the input order of the BDD does not much affect the overall size of the BDD, which is similar to the BDDs in the AES implementation [7].

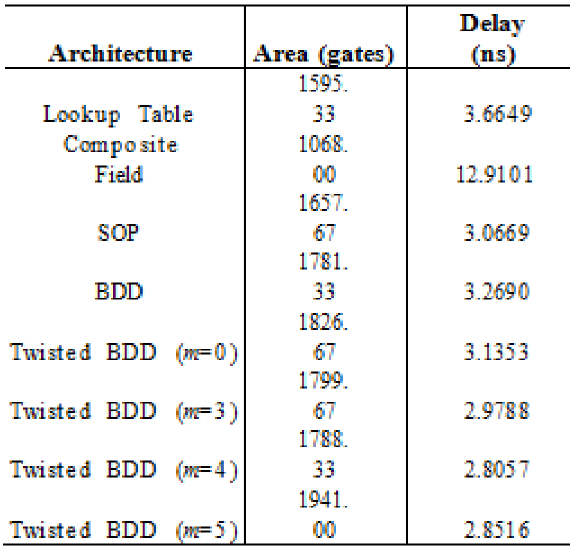
In addition, an exhaustive search for the smallest.

Table II. Comparison of Various Sms4 S-Box Architectures on Smic 0.18µm Cmos Technology



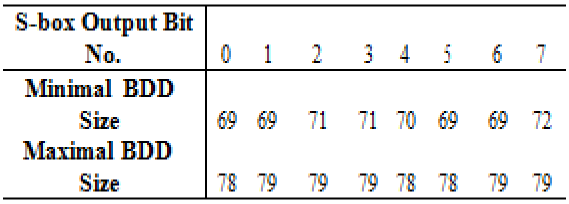
Architecture	Area (gates)	Delay (ns)
Lookup Table	1640.67	1.9409
Composite Field	1321.33	6.7263
SOP	1690.33	1.6786
BDD	1795.67	1.7628
Twisted BDD (*m*=0)	1975.00	1.6765
Twisted BDD (*m*=3)	2092.33	1.6180
Twisted BDD (*m*=4)	2097.33	1.5326
Twisted BDD (*m*=5)	2206.33	1.6087

Table III. Comparison of Various Sms4 S-Box Architectures on Chartered 0.35µm Cmos Technology



Architecture	Area (gates)	Delay (ns)
Lookup Table	1595.33	3.6649
Composite Field	1068.00	12.9101
SOP	1657.67	3.0669
BDD	1781.33	3.2690
Twisted BDD (*m*=0)	1826.67	3.1353
Twisted BDD (*m*=3)	1799.67	2.9788
Twisted BDD (*m*=4)	1788.33	2.8057
Twisted BDD (*m*=5)	1941.00	2.8516

TABLE IV.BDD SIZE RANGES



S-box Output Bit No.	0	1	2	3	4	5	6	7
Minimal BDD Size	69	69	71	71	70	69	69	72
Maximal BDD Size	78	79	79	79	78	78	79	79

Fastest twisted BDD architecture will consume much time, because the total number of the possible input orders combinations of the 8 BDDs in the twisted BDD architecture is 8!×7!=203,212,800.

So, we have not done any optimization about input orders of the BDDs. The input order combination selected in our SMS4 VLSI implementation and the sizes of the BDDs are shown in Table V. Also, the 4 levels at the input side of each BDD, which correspond to the (8–*m*) inputs at the input side in Fig. 2 where *m*=4, are also shown in Table V.

TABLE V. INPUT ORDERS AND SIZES OF BDDS IN SMS4 VLSI IMPLEMENTATION

S-box Output Bit No.	Input Order ($in_7...in_0$)	BDD Size (Full)	BDD Size (4 Levels at Input Side)
0	(01234567)	74	59
1	(12345670)	78	63
2	(23456701)	74	59
3	(34567012)	78	63
4	(45670123)	76	61
5	(56701234)	77	62
6	(67012345)	72	57
7	(70123456)	78	63

B. *Implementation Results*

On SMIC 0.18μm technology and Chartered 0.35μm technology, we completed the RTL coding, logic synthesis and physical design of the full SMS4 cipher VLSI design with the twisted BDD S-box architecture with *m*=4. The implementation results are shown in Table VI, including the area, the delay, the maximal frequency and the throughput in the cipher block chaining (CBC) mode.

In the SMS4 VLSI implementation, we achieved a frequency more than 200MHz and a throughput more than 800Mbps on SMIC 0.18μm technology, and a frequency more than 100MHz and a throughput more than 400Mbps on Chartered 0.35μm technology.

IV. DISCUSSION

Based on twisted BDD architecture, we improved the operation speed of the S-box circuit and also the full SMS4 cipher VLSI design. On the other hand, from the implementation results, we can find that much of the critical path delay is used by other operations other than S-box, including XORs, multiplexors and setup time required by the technology. So, future works on improving the SMS4 circuit speed can be focused on the fast circuit architecture design of other parts in SMS4 cipher.

V. CONCLUSIONS

In this paper, we evaluated several circuit architectures of the S-box in SMS4 cipher and completed a fast full SMS4 cipher VLSI implementation based on the twisted BDD S-box architecture with *m*=4. According to the experiment results, our SMS4 circuit can run at speeds over 200MHz on SMIC 0.18μm technology and over 100MHz on Chartered 0.35μm technology, and achieves over 800Mbps and 400Mbps throughputs in the CBC mode respectively. The design presented in this paper is suitable for the application fields that require a high operation speed and throughput.

Fastest twisted BDD architecture will consume much time, because the total number of the possible input orders combinations of the 8 BDDs in the twisted BDD architecture is 8!×7!=203,212,800.

So, we have not done any optimization about input orders of the BDDs. The input order combination selected in our SMS4 VLSI implementation and the sizes of the BDDs are shown in Table V. Also, the 4 levels at the input

side of each BDD, which correspond to the (8–*m*) inputs at the input side in Fig. 2 where *m*=4, are also shown in Table V.

REFERENCES

[1]. Office of State Commercial Cipher Administration of China, "SMS4 cipher for WLAN products (in Chinese)," 2006. [Online]. Available: http://www.oscca.gov.cn/UpFile/200621016423197990.pdf

[2]. X. Bai, L. Guo, and T. Li, "Differential power analysis attack on SMS4 block cipher," in *Proceedings of 4th IEEE International Conference on Circuits and Systems for Communications, ICCSC 2008*, Shanghai, China, May 2008, pp. 613–617.

[3]. L. Zhang and W. Wu, "Differential fault analysis on SMS4 (in Chinese)," *Chinese Journal of Computers*, vol. 29, no. 9, pp. 1596– 1602, 2006.

[4]. W. Li and D. Gu, "An improved method of differential fault analysis on the SMS4 cryptosystem," in *Proceedings of 1st International Symposium on Data, Privacy, and E-Commerce, ISDPE 2007*, Chengdu, China, Nov. 2007, pp. 175–180.

[5]. F. Liu, W. Ji, L. Hu, J. Ding, S. Lv, A. Pyshkin, and R.-P. Weinmann, "Analysis of the SMS4 block cipher," in *Information Security and Privacy, 12th Australasian Conference, ACISP 2007, Proceedings, LNCS 4586*, Townsville, Australia, Jul. 2007, pp. 158–170.

[6]. Y. Jin, H. Shen, and R. You, "Implementation of SMS4 block cipher on FPGA," in *Proceedings of 1st International Conference on Communications and Networking in China, ChinaCom'06*, Beijing, China, Oct. 2006, pp. 1–4.

[7]. S. Morioka and A. Satoh, "A 10-Gbps full-AES crypto design with a twisted BDD S-box architecture," *IEEE Trans. VLSI Syst.*, vol. 12, no. 7, pp. 686–691, Jul. 2004.

[8]. U. Mayer, C. Oelsner, and T. Köhler, "Evaluation of different Rijndael implementations for high end servers," in *Proceedings of 2002 IEEE International Symposium on Circuits and Systems, ISCAS 2002*, vol. 2, Scottsdale, AZ, USA, May 2002, pp. 348–351.

[9]. F. Somenzi, "CUDD: CU decision diagram package release 2.4.1," 2005. [Online]. Available: http://vlsi.colorado.edu/~fabio/CUDD