Proceedings of the International Conference on Intelligent Computing and Communication for Smart World (I2C2SW-2018)
14-15 December 2018

In Depth Survey on SMS4 Architecture

M. Babu
Department of ECE
RMK College of Engineering and technology
Chennai, India
ibabum@gmail.com

G. A. Sathish Kumar
Department of ECE
Sri Venkateswara Engineering College
Chennai, India
sathish@svce.ac.in

***Abstract*— In the present world, securing data is very necessary in every industry especially in defense sector and banking sector. Many encryption algorithms are proposed to prevent the data theft. In this paper various architectures of SMS4 algorithm is discussed. SMS4 is a Chinese standard cipher developed for securing information in Wireless Local Area Network (WLAN). This survey is done to propose a new modified SMS4 architecture, which can perform secure encryption and decryption better than the existing SMS4 architectures. Finally discussed about the possible ways of changes can be done for improvement.**

Keywords—DPA, LUT, SMS4, Twisted BDD, ESMS4

I. INTRODUCTION

Information through wireless medium is prone to hacking. There exists two types of intruders, intentional intruders and non-intentional intruders. Former one will be very keen in stealing the data from secured channel and create a big threat to sender. Their ultimate aim is to crack the cipher text [13] and to get the plain text [13], which contains the secret information. The latter one is who get to know the secrecy over the secured channel accidentally. Even though it is not a major issue, we have to consider both attacks while designing an encryption [13] algorithm.

Now a days hacking becomes a fashion and many licensed and unlicensed hackers are trying to steal the private data over wireless environment. Only with the help of strong encryption algorithm can prevent this data theft and can give necessary secrecy.

According to SANS [14], Julius Caesar is considered to be the first person who used an encryption standard to secure the message transaction. The scheme used by him is known as Caesar cipher. Cryptanalysis [13] becomes a tedious task if the algorithm used to encipher the message is powerful.

SMS4 [1] is a Chinese standard encryption algorithm. It is a 128-bit block cipher developed to protect data packets in WLAN. SMS4 basic architecture is explained in [1] and [12]. Both encryption and decryption contains 32 rounds. 128 bits of input is split into four 32-bit and processed. In each round, plain text is processed with round key first, followed by transformation box. Transformation is of two steps: linear and non-linear. In non-linear transformation, data is processed through S-boxes (Substitution boxes). Various S-box architectures are discussed in the following sections. In former case, data is shifted linearly to introduce confusion in encrypted text. Here key generation and encryption are happening at the same time. Plain text and Cipher text are part of (GF(232))4. Key is part of GF(232).

Main objectives of cryptography are authentication and privacy.SMS4 is such type of cipher which provides both authentication and privacy in wireless medium. Wireless medium is commonly a non-secured public channel and providing privacy in it is a bigger challenge. Anybody in the network can get the encrypted message from the medium. Increasing the difficulty in decrypting the same is the success behind every cryptographic algorithm. Symmetric key algorithms, like SMS4, uses same keys for both encryption and decryption. Unlike other algorithms, in SMS4 key is computed from the plain text to be encrypted while encryption and from cipher text while decryption. So there is no additional transmission of keys to the receiver is required. And also architecture used for encryption / decryption.

Privacy of the message is achieved in SMS4 by means of two steps, one is by confusion and second one is by diffusion. Both process are taking place in transformation block in each round. Transformation consists of non-linear S-box transformation and linear cyclic left shift transformation. Confusion process is carried out in non-linear transformation block and diffusion process in linear transformation block. Sections 2,3and 4 are discussing about non-linear transformation block design in which the design using Twisted BDD S-Box with m=4 is proved to be the fastest one than other architectures surveyed. Section 5, 6 and 7 are dealing with various attacks performed on SMS4 and the modified designs to overcome those attacks.In this paper, various SMS4 cipher architecture is surveyed and discussed about the possibilities to improve further.

II. LUT S-BOX SMS4

Look Up Table (LUT) S-Box architecture is discussed in [1] and [12]. In this S-box architecture a LUT is used for encryption as well as decryption. Values in the LUT are determined in the initial stage itself. S-box can handle 32 bits of data at a time. Since there are 4 S-boxes, each can handle 8 bits at a time. Out of these 8 bits, first 4 bits represents the row and the remaining 4 represents column in the LUT. Same process is taken places in other S-boxes also. SMS4 using LUT architecture achieved 1.94ns delay and 1640 gates while implementing with 0.18µm CMOS (Complementary Metal Oxide Semiconductor) technology, 3.66ns delay and 1595 gates with 0.35µm technology [1] and 6.6ms delay and 1.03GB storage space with 0.5µm technology [12]. Figure 1 and 2 show the graphical representation of area utilization and delay respectively

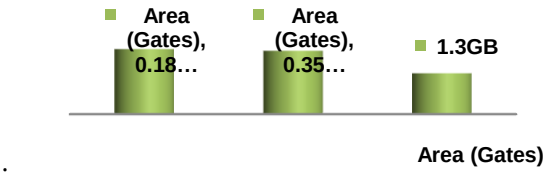

Fig. 1. Area utilization of LUT S-Box design

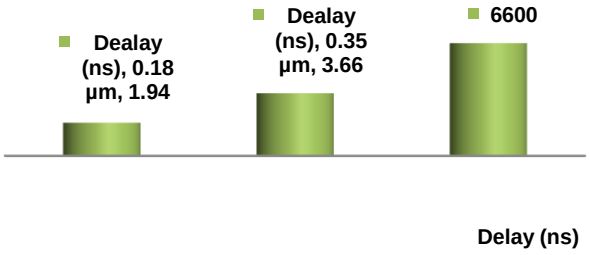

Fig. 2. Delay of LUT S-Box design

III. BDD S-BOX SMS4

XusfeiBaiet. al have discussed about BDD (Binary Decision Diagram) S-box architecture in [1]. BDD contains (8-m) inputs encoder and an m to 2m decoder. Both encoding and decoding happened simultaneously to generate S-box output. By varying the value of m, different delay can be achieved in encryption and decryption process. SMS4 BDD s-box architecture achieved 1.76ns delay and 1795 gates in 0.18µm CMOS technology and 3.27ns delay and 1781 gates in 0.35µm technology [1]. Figure 3 shows Delay and Area utilization.

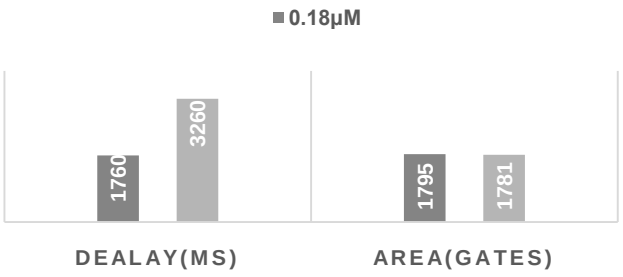

Fig. 3. Delay and Area utilization of BDD S-Box design

IV. TWISTED BDD S-BOX SMS4

Babu et. al have discussed Twisted BDD S-box architecture in [12]. In Twisted BDD architecture, 8 BDD structures are arranged in parallel to process the data. Each BDD has (8-m) input encoders and m to 2m decoders. By varying m value from 0 to 5, six different architectures of Twisted BDD were analyzed [12] (ie, m=0, m=1, m=2, m=3, m=4 and m=5) and proved that architecture with m=4 is faster than other architectures [1]. Figure 4 shows Delay and Area utilization.

V. PIPELINED SMS4

Babuet. al have proposed pipelined SMS4 [12] architecture. Pipelining is the process used to improve the performance of the architecture. Two stage pipelining is implemented in this paper by adding buffers in data path. Buffer is inserted after the linear transformation block. The 32 bit LSB data and 32 bit linear transformation data are fed to the buffers before XORing. These buffers can be implemented with any of the data structure. Queue is considered for the proposed design. This paper proved that pipelined SMS4 architecture is faster than LUT, BDD [1] and Twisted BDD [12] architectures. Figure 5 shows Delay and Memory usage.

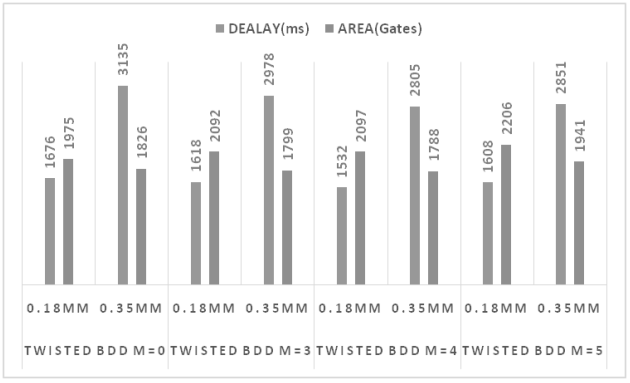

Fig. 4. Delay and Area utilization of Twisted BDD S-Box design

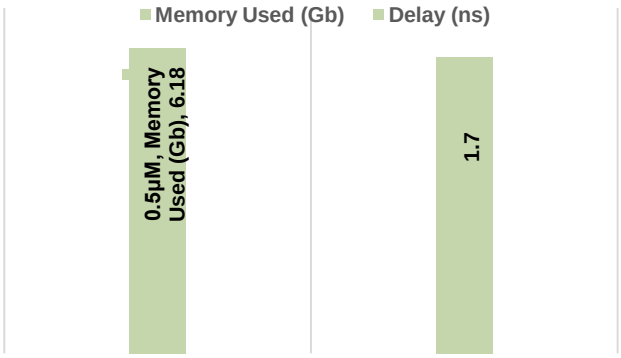

Fig. 5. Delay and Memory usage of Pipelined SMS4

VI. SMS4 – GCM

Meng Zhao et al have proposed SMS4-GCM [11] architecture. Galios Counter Mode (GCM) is an operating mode of high speed block cipher. Full pipelined architecture is used to design SMS4-GCM architecture. Compared to SMS4-pipelined architecture, in SMS4-GCM pipelining is applied in every rounds. This structure helped to reduce data processing delay that the data from previous round get stored in the buffer and readily available for the transformation blocks of next round. Average processing speed is around 32 times larger than the SMS4 architecture. This paper achieved high efficiency encryption and authentication with processing rate of 22.248Gbps.

VII. ROLLING AND UNROLLING SMS4

XianweiGao et. al have designed and implemented rolling and unrolling architectures [8] of SMS4 cipher. Former one transforms data iteratively by using a feedback structure and also used a control circuit to take care of the flow of encryption with the help of Finite State Machine (FSM). Latter one uses a 32 level pipelined architecture. Because of the simultaneous action of all the 32 registers, the first cipher text is obtained after 32 clock cycles, second cipher text is

TABLE I. COMPARISON OF VARIOUS SMS4 ARCHITECTURES

Architecture	Delay	Area	Allotted Resources	Speed / Throughput	Authentication	Power Consumption	Hardware Cost	Security	Complexity
LUT S-Box SMS4	1.94 ns	1640 gates	380	-	-	-	-	-	HIGH
BDD S-Box SMS4	1.76 ns	1795 gates		-	-	-	-	-	HIGH
Twisted BDD S-Box SMS4	1.5 ns	2097 gates		-	-	-	-	-	HIGH
Pipelined SMS4	1.7 ns	6.18 GB		-	-	-	-	-	HIGH
SMS4-GCM	-	-	-	22.248 Gbps	YES	-	-	-	HIGH
Rolling & Unrolling SMS4	-	-	-	32 rounds/ Clock cycle	-	-	-	-	HIGH
SEC-PROC SMS4	-	-	289	-	-	-	-	-	HIGH
Folded & Reconfigurable SMS4	-	22k gates	-	6.3 Gbps	-	-	-	-	HIGH
DPA Resistant SMS4	-	22k gates	-	-	-	LESS	LESS	YES	HIGH
Optimized SMS4	-	-	-	-	-	LESS	LESS	YES	HIGH
ESMS4	-	-	-	-	-	LESS	LESS	YES	LOW

obtained at the 33rd clock cycle, third one at the 34th clock cycle and so on. So, average clock cycle required to obtain a 128-bit cipher text is only one. Thus the architectures improved speed and throughput.

VIII. SEC – PROC SMS4

Nicolas et. al have proposed SECurity standard co-PROCessor (SEC-PROC) [9] SMS4 cipher designed for achieving security in WLAN. The paper mainly concentrated on architectural optimization of SMS4 cipher. Resource allocation of SEC-PRO SMS4 is compared with standard SMS4[1] and proved that proposed architecture uses only less resource. SEC-PROC SMS4 uses 289 allocated resources but SMS4 uses 380.

IX. FOLDED AND RECONFIGURABLE SMS4

Bo Wang et. al have introduced a reconfigurable crypto [10] SMS4 architecture. Inter Connection Tree between Rows (ICTR) optimization method and Hierarchical Context Optimization methods (HCO) are proposed. This paper achieved efficiency in area and energy and also achieved a throughput of 6.3Gbps.

Weiei Yan et. al have proposed a folded and reconfigurable SMS4 architecture [2]. Total gates used for the implementation is only 22k gates. If number of gates required for the design is less, area also reduced, consequently cost also reduced.

X. DPA RESISTANT SMS4

XuefeiBaiet. al proved that SMS4 architecture is prone to Differential Power Analysis (DPA) attack [15]. DPA is considered to be the efficient side channel attack, which uses the statistical analysis of power dissipation during processing.

Improved SMS4 with masking [5] is proposed to improve security against DPA attack. Masking scheme is implemented with respect to composite field arithmetic in which inversion is shifted from $GF(2^8)$ down to $GF(2^2)$. By reusing modules and by changing the order of computation, tried to reduce area but it could not achieve the area reduction than folded reconfigurable architecture. 25k gates are used in improved SMS4 structure.

Masking is of two types. Fixed value masking and Random value masking. Fixed value masking algorithm is proposed [7] to prevent DPA attack. This algorithm requires only less RAM capacity and faster than the latter. Masking is applied to both linear and non-linear transformation blocks of the SMS4 architecture.

Chen Yichenget. al have proposed a method to prevent DPA attack by combining masking and power randomization techniques [6]. Masking and power randomization are applied to the linear transformation block and non-linear transformation block respectively. The power consumption of the process is independent of the immediate values and thus this approach is economical.

Jiachao Chen et. al have proposed combined hiding and masking [4] to secure data against chosen plain text attack. Random masking is employed in linear transformation block and fixed masking in non-linear transformation block. Pseudo rounds are also used to improve security against DPA.

XI. OPTIMIZED SMS4

Lin Han et. al have proposed an optimized SMS4 architecture [3] to reduce power consumption and hardware cost. The proposed architecture used 3 stage pipelining and generation of pseudo round keys for securing its storage in

shared memory. A secure programmable processor hardware implementation is done in this paper.

XII. ESMS4

As discussed in section 1, SMS4 has a block size of 128bit and is processed by splitting into four words each of 32 bits. Last three words are EXOR-ed with round key in each round and is processed in transformation block. S-box non-linear transformation block and linear transformation block and linear transformation block operate over $GF(2^8)$ and GF(2) respectively. Over the field $GF(2^8)$, inversion transformation of S-box takes place and over GF(2), cyclic shift towards left takes place. Thus transformation block in SMS4 operates over two fields. This makes cryptanalysis complicated. To avoid this complexity ESMS4 is proposed [16]. ESMS4 is an extended version of SMS4 in which transformation block operates over a single field $GF(2^8)$. A multiplicative quadratic equation over $GF(2^8)$ also described in [16]. The values obtained after key mixing are considered as the elements of field $GF(2^8)$. Vector space of SMS4 is $GF(2^8)^4$ and is denoted as $\mathcal{A}$ and the vector space of ESMS4 is $GF(2^8)^{32}$ and is denoted as □ Vector space of ESMS4 can be obtained by doing conjugate mapping of vector space in SMS4 as mentioned in equation 1.

$$\mathcal{E} = \emptyset(\mathcal{A}) \quad (1)$$

The vector conjugate transform follows additive property and also inversion property, for example

for any $x=(x_0,x_1,\ldots,x_{n-1}) \in GF(2^8)^n$ (2)

$$\emptyset'(x) = (\emptyset(x_0),\emptyset(x_1),\ldots,\emptyset(x_{n-1})) \quad (3)$$

$$\emptyset'(x+x') = \emptyset'(x)+\emptyset'(x') \rightarrow \text{additive property} \quad (4)$$

$$\emptyset'(a^{(-1)}) = \emptyset'(a)^{-1} \rightarrow \text{inversion property} \quad (5)$$

By using these properties state vector of SMS4 is embedded into SMS4. The EXOR operation and inversion operation in the transformation process is extended from GF(2) to $GF(2^8)$. Complexity calculated is 2^{77}.

XIII. DISCUSSION AND CONCLUSION

Table 1 shows the comparison made according to the survey of various SMS4 architectures. This survey is done to study about the various possibilities to improve the performance of the architecture of SMS4 cipher algorithm. In WLAN, protecting the data packets is a crucial task. As discussed in section I, to secure the data from intruders, new algorithm must be more complex and at the same time it should be easy to be decrypted by the intended receiver. And also, without using a separate architecture, both encryption and decryption process have to be carried out simultaneously without any processing delay. Implementation of pipelining can be considered in key generation stage also.

The efficient design of XOR gate can be taken care to improve the area and speed of encryption and decryption. Normally XOR gates are implemented using standard CMOS logic. Some other logics can be adopted. In SMS4 architecture [1], 128 bit data is split into four 32 bits and processed. This can be further divided and processed using some other approach to improve complexity and thus to improve security. Confusion and diffusion are mainly taken place in transformation blocks in SMS4 architecture [1][12]. Both the processes can be used in different parts of the architecture.

The main objective in the future work will be manly focusing on speed processing, increasing complexity towards different attacks, easing encryption and decryption process and improving secrecy of the data.

REFERENCES

[1] XuefeiBai, Li Guo, Lu Huang, and YanhuaXu, "A Fast VLSI Design of SMS4 Cipher Based on Twisted BDD S-Box Architecture", International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 345-348, 978-0-7695-3610-1/09 $25.00 © 2009 IEEE.

[2] Weiwei Yan, Kaidi You, Jun Han and XiaoyangZeng, "Low-Cost Reconfigurable VLSI Implementation of the SMS4 and AES Algorithms", pp. 135-138, 978-1-4244-3870-9/09/$25.00 ©2009 IEEE.

[3] Lin Han, Jun Han, XiaoyangZeng, Ronghua Lu, Jia Zhao, "A Programmable Security Processor for Cryptography Algorithms", 978-1-4244-2186-2/08/$25.00 ©2008 IEEE.

[4] Jiachao Chen, Qin Wang, ZhengGuo and Junrong Liu, "A Circuit Design of SMS4 against Chosen Plaintext Attack, 11th International Conference on Computational Intelligence and Security", pp.371-374, 978-1-4673-8660-9/15 $31.00 © 2015 IEEE.

[5] XuefeiBai, YanhuaXu and Li Guo, "Securing SMS4 Cipher against Differential Power Analysis and Its VLSI Implementation", pp. 167-172, 1-4244-2424-5/08/$20.00 © 2008 IEEE.

[6] Chen Yicheng and ZhengZhaoxia, "Design and Implementation of Power Analysis immune SMS4 Algorithm".

[7] XiaoyiDuan, Ronglei Hu and XiuYing Li, "Research and Implementation of DPA-resistant SMS4 Block Cipher", Seventh International Conference on Computational Intelligence and Security, pp.1034-1036, 2011.

[8] XianweiGaoErhong Lu Liqin Xian Hanlin Chen, "FPGA Implementation of the SMS4 Block Cipher in the Chinese WAPI Standard", International Conference on Embedded Software and Systems Symposia, pp. 104-106, 978-0-7695-3288-2/08 $25.00 © 2008 IEEE.

[9] Nicolas Sklavos and Paris Kitsos, "Architectural Optimizations & Hardware Implementations of WLANs Encryption Standard", 978-1-4673-0229-6/12/$31.00 ©2012 IEEE.

[10] Bo Wang and Leibo Liu, "A Flexible and Energy-Efficient Reconfigurable Architecture for Symmetric Cipher Processing", pp. 1182-1185, 978-1-4799-8391-9/15/$31.00 ©2015 IEEE.

[11] Meng Zhao, GuochuShou, Yihong Hu and ZhigangGuo, "High-Speed Architecture Design and Implementation for SMS4-GCM", Third International Conference on Communications and Mobile Computing, pp. 15-18, 978-0-7695-4357-4/11 $26.00 © 2011 IEEE.

[12] Babu M, Mukuntharaj C and Saranya S, "Pipelined Sms4 Cipher Design for Fast Encryption Using Twisted BDD S-Box Architecture", International Journal of Computer Applications & Information Technology, Vol. I, Issue III, November 2012, pp. 26-30, ISSN: 2278-7720.

[13] https://en.wikipedia.org/wiki/History_of_ cryptography.

[14] https://www.sans.org/readingroom/whitepapers/vpns/history-encryption-730.

[15] XuefeiBai, Li Guo and Tie Li, "Differential Power Analysis Attack on SMS4 Block Cipher", pp. 613-617, 978-1-4244-1708-7/08/$25.00 ©2008 IEEE.

[16] Ji W., Hu L. (2007) New Description of SMS4 by an Embedding over $GF(2^8)$. In: Srinathan K., Rangan C.P., Yung M. (eds) Progress in Cryptology – INDOCRYPT 2007. Lecture Notes in Computer Science, vol 4859. Springer, Berlin, Heidelberg