IPHV8I1003X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

AES ALGORITHM FOR HIGH SPEED FAULT DETECTION

[#1]MUDRABOINA SAMBARAJU – Pursuing M.Tech,
[#2]P.NARASIMHULU - Associate Professor,
SREE CHAITANYA COLLEGE OF ENGINEERING, KARIMNAGAR, T.S., INDIA.

ABSTRACT: Cryptography is a method that has been developed to ensure the secrecy of messages and transfer data securely. Advanced Encryption Standard (AES) has been made as the first choice for many critical applications because of the high level of security and the fast hardware and software implementations, many of which are power and resource constrained and requires reliable and efficient hardware implementations. Naturally occurring and maliciously injected faults reduce the reliability of Advanced Encryption Standard (AES) and may leak confidential information. In this paper, a lightweight concurrent fault detection scheme for the AES is presented. In the proposed approach, the composite field S-box and inverse S-box are divided into blocks and the predicted parities of these blocks are obtained. For high speed applications, S-box implementation based on lookup tables is avoided. Instead, logic gate implementations based on composite fields are utilized. A compact architecture for the AES Mix-columns operation and its inverse is also presented. This parity-based fault detection scheme reaches the maximum fault coverage when compared to other methods of fault detection. The proposed fault detection technique for AES encryption and decryption has the least area and power consumption compared to their counterparts with similar fault detection capabilities. In the proposed approach, the composite field S-box and inverse S-box are divided into blocks and the predicted parities of these blocks are obtained. By using exhaustive searches We obtained the optimum solutions for the least overhead parity-based fault detection structures. It suggests both the ASIC and FPGA implementations of the fault detection structures using the obtained optimum composite fields, have better hardware and time complexities compared to their counterparts.

Index Terms: ***AES, composite fields, parity prediction, fault detection, S-box.***

I.INTRODUCTION

The Advanced Encryption Standard (AES) has been accepted by NIST [1] as the symmetric key standard as a replacement for the previous standards because of its good characteristics in terms of secur ity, cost, and efficient implementations for encryption and decryption of blocks of data. In encryption, under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. AES may be configured to use different key-lengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key. After 10 rounds, the cipher text is generated where each encryption round (except for the final round) consists of four transformations. The four transformations of round of encryption are explained below.

The 128 bits of input (and output) of each transformation are considered as a four by four matrix, called state, whose entries are eight bits. Except for the last round, the first transformation in each round is the bytes substitution, called SubBytes, which is implemented by 16 S-boxes. Shift-Rows is the second transformation in which the four bytes of the last three rows of the input state are cyclically shifted. The third transformation is Mixcolumns in which the columns are considered as polynomials over GF(28) and multiplied by a fixed polynomial. The final transformation is AddRoundKey in which a roundkey is added to the input by 128 two- input XOR gates.

Among the transformations in the AES, the S-boxes in the encryption and the inverse S-boxes in the decryption are alone nonlinear. Fault detection in the AES hardware implementation is important in order to make the standard robust to the internal and malicious faults. There exists various fault detection schemes for the AES hardware implementation. For fault detection of the encryption or decryption in AES redundant units may be used [12], [14], where algorithm-level, round-level and operation-level concurrent error detection for the AES is used. A number of fault detection schemes based on the error detecting codes, also exists. For high performance AES implementations, using ROMs may not be preferable. The proposed fault detection approach is applied to the composite field AES encryption and decryption. There exist a number of fault detection approaches which are specific to composite field S-boxes and inverse S-boxes. In the scheme of [13], the fault detection of the multiplicative inversion of the S-box is considered. In [12], predicted parities have been used for the multiplicative inversion of a specific S-box using composite field and polynomial basis.

IPHV8I1003X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Furthermore, the transformation matrices are also considered. In [12] and [6], the composite field S-boxes and inverse S-boxes (using polynomial basis) have been divided into sub-blocks and parity predictions are used for their fault detection.

In the schemes proposed in [15] and [22], all the search space of composite fields is considered for presenting optimum lightweight fault detection schemes. The scheme presented in [8] is for all the transformations in the AES encryption/decryption independent of the ways these transformations are implemented. Moreover, the scheme presented in [7] uses double-data-rate computation for counteracting the fault attacks. Additionally, a fault detection scheme based on the Hamming and Reed-Solomon codes for protecting the storage elements within the AES is proposed in [11]. It is also noted that, for the logic elements, the scheme in [2] and the use of the partial duplication of the most vulnerable elements are proposed in [11].

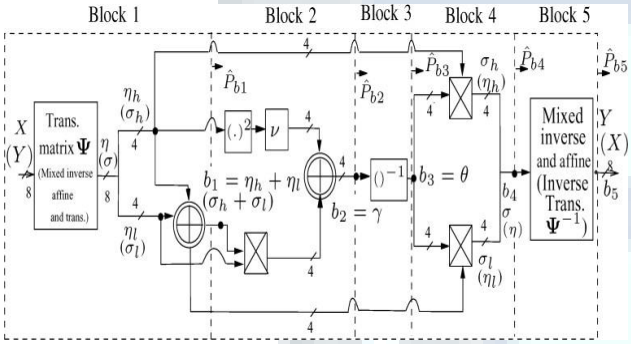

Fig. 1. The S-box (the inverse S-box) using composite fields and polynomial basis and their fault detection blocks.

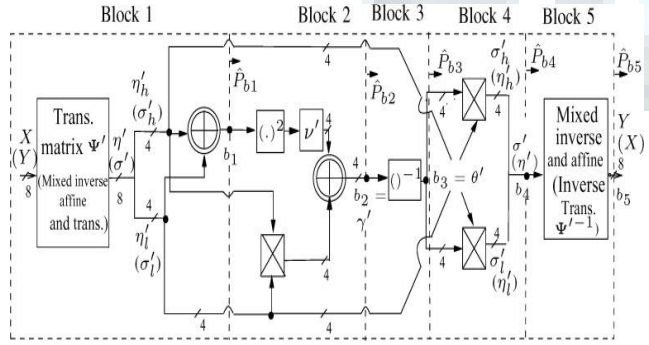

Fig. 2. The S-box (the inverse S-box) using composite fields and normal basis and their fault detection blocks.

All the S-boxes (respectively the inverse S-boxes) occupy much of the total AES encryption (respectively decryption) area and their power consumption is around three fourths of that of the entire AES [16]. LUTs can be utilized for the AES S-boxes and inverse S-boxes in hardware implementation. This work involves low-area implementation of the AES encryption and decryption using composite fields.

The contributions of this paper are as follows.

- The S-box and the inverse S-box has been designed to obtain low power and low area.
- An alternative lightweight design for both forward and inverse mixcolumns operation required in the AES hardware implementation is also presented.
- A low-cost parity-based fault detection scheme for the S-box and the inverse S-box using composite fields is presented, for increasing the error coverage. The predicted parities of the five blocks of the S-box and the inverse S-box are obtained (three predicted parities for the multiplicative inversion and two for the transformation and affine matrices).
- The actual parity is obtained from the blocks using XOR gates. The predicted parity is compared with the actual parity. The error gets indicated using the error indication flag.
- The proposed fault detection scheme is simulated and maximum error coverage is obtained compared to existing methods. It is shown that the power and area of the proposed technique is least compared to the schemes that have the same fault detection capabilities.

II. RELATED WORKS

In [1], one of the best symmetric security algorithms is used to provide data security in AES. The pipelined architecture of the AES algorithm increases the throughput of the algorithm and the pipelined key schedule algorithm increases the speedup. In this architecture, instead of passing the output of each round to the next round directly, a register is used. It avoids the direct contact between two rounds. With the help of search based Look-Up-Table, the hardware cost is reduced. The speed of the AES algorithm is increased by inserting compact and flexible architecture for Mix Column transform. In [2], a fixed coefficient multiplier for Mix Column operation and an equivalent pipelined architecture leads to effective utilization of resources and increase in speed. The modifications in each round of the AES algorithm in [3], improved the complexity of the encryption method and making it complicated for the attacker to predict a pattern in the algorithm. In each transformation of the modified architecture, the 8-bit values are separated in to 4-bits and they are grouped and then perform the transformation process. The modifications have provided the algorithm with strong diffusion and confusion. A high data throughput AES hardware architecture is proposed in [4] by partitioning the 10 rounds into sub blocks of repeated AES modules. To provide a complete ten stages of AES, the intermediate buffers are used to separate the blocks. Using this pipelined architecture scheme, time complexity is reduced to greater extent. In [5], a simple, linear and cryptanalysis is done on the standard S-Box to take advantage of high probability occurrences of linear expressions involving plain text bits , cipher text bits and sub-key bits. The operation of the cipher is linear

where the linearity refers to a mod-2-bitwise operation. The design can run at 1.2 GHz which is sufficient for online data encryption. The Mix Column in [6] could be designed easily using one basic module which imposes one time block, two or three byte-XOR logic and additional data path selector. The optimized architecture of data encryption unit and key schedule unit is applicable to wireless sensor networks. In [7], a 128-bit AES encryption and decryption using Rijndael Algorithm is designed and synthesized using verilog code which can be easily implemented with the help of FPGA. The design and performance testing algorithm in [8] is implemented with the help of dynamic partially reconfigurable FPGA. To self select the coprocessors, a FPGA based Micro-Blaze processor is used which reduces area requirements and increase system's versatility. To increase the performance of the executed circuit, particularly cost and power, all of the AES blocks may be reconfigurable. So the parameters used for reconfiguration are implanted inside the manager module of reconfiguring, and also possible to quickly cross from a safe configuration to another by updating a hard system protection.

III. FAULT INJECTION, DETECTION AND RECTIFICATION

From the previous implementations, the Fault Detection scheme is mainly based on Parity Checking method where the actual parity is compared with predicted parity with OR Gates which is used for error detection [15]. The actual drawback in this condition is the OR Gate generated erroneous output which reduced the Fault Coverage to 97%.In Reconfigurable Architecture [1], the cells have been portioned into 4 x 4 matrix with the parity bits and the output parity is compared with the input parity and the faulty cell is being replaced with the neighbor cell with routing scheme which offers the reconfigurable architecture and increases the Fault coverage to 98% by increasing the area. In Low Overhead Parity Scheme, the S-Box is divided into 5 blocks and this offers 97% of the Fault coverage approach for multibit parity prediction. [12].In parallel AES technique, the on-line fault detection scheme is based on functional redundancy [9] where the sub-blocks which are repeated are partioned and compared with on line fault detection scheme where the faults are injected by side channel attacks and the fault detection probability is found to be 99.9%. In single fault masking technique of a Dual Port Ram, a part of the hardware is used for Parity Checking where the basic advantage of this method is it requires no extra clock and it requires no extra FPGA RAM blocks and the fault coverage is found to be 100% [20]. Here we consider the Differential Faults in terms of Hardware Fault Analysis and introduce a new concept of Component Reusability which never uses the spare of the original. Reusability means one faulty behavior of one circuit exactly matches the behavior of a faultless circuit the first faulty circuit can replace the second circuit whenever the second circuit becomes faulty without the need to go for a spare circuit. It is a method of Testing and the best applications of Fault Tolerant Design. By this method, we can save the hardware resources and make the system to shoot up immediately in case if a Fault is detected. Here we consider the Fault in the S-Box during the cyclic shift operation where each cell in the S-Box contains 8 bits and is designed with the help of multiplexers which performs the Left Rotate operation. The Differential Fault is injected using Fault Injection Circuits which leads to Component Malfunction so that the S-Box becomes faulty as shown below in TABLE

1where the Faulty Operations are indicated by RED Color. In this method, we are specifying the fault at a particular location by the user defined module to the inputs. Consider the 8 To 1 Multiplexer shown below in Figure10 which is used for the design of rotator.

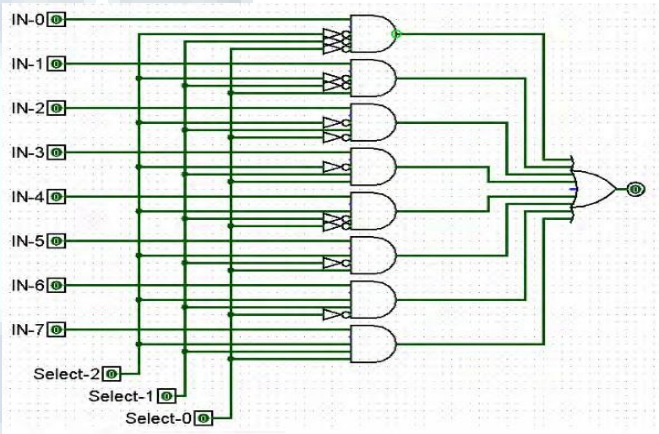

Figure 10: Multiplexer Unit used for Rotator of AES Module

Suppose if the AND Gate connected to the IN-0 input fails, then the following modules will be malfunctioning based on the Control Signals shown below in RED Color in TABLE 1.

Control Signal	Operation	S-Box Operation			
000	No Change	a0,0	a0,1	a0,2	a0,3
001	Left Rotate 1	a1,1	a1,2	a1,3	a1,0
010	Left Rotate 2	a2,2	a2,3	a2,0	a2,1
111	Left Rotate 3	a3,3	a3,0	a3,1	a3,2

TABLE 1: Faulty S-BOX Unit for AES Module

Once the Fault has been indicated during the normal rotate operation, we have to use the shortest routing path to connect to the alternate hardware which has the same operation of the faulty one so that this will overcome the faulty circuit to reduce the delay in the operation which enhances the speed of the circuit operation. For exampleas indicated if the AND Gate connected to the IN-0 input fails, we can use the AND Gate connected to the IN-1 to provide the exact output for IN-0 as due to similarity of the components connected. By this method, we can use the component reusability technique, a new

method in VLSI Testing and save the hardware resources. In this case once the fault is identified, the particular hardware is identified and instead of creating a duplicate / spare of it, we can use the other working component whose function is similar to the faulty one and make the resource to work perfectly thus saving time.

V. IMPLEMENTATION RESULTS

When analyzed with the previous implementations, they use Parity Bit scheme which verifies the parities at both the ends and requires more complexity in designing the scheme and the Fault coverage Efficiency is found to be 97% - 98%. Our implementation shows 100% Fault correction Capability where the given hardware itself acts as an auto corrector which uses the principle of Fault Tolerant Routing and also overcomes the previous methods of adding Parity Bits and never use spare components. The mean time required to resume a component takes 3 clock cycles as to input the test vectors to the nearest component which has the same operation of the failed component and to make the component to start exactly from the last input as when the fault occurred. The design has been taken high consideration in terms of low power, area and throughput for high frequency and to obtain high Fault coverage and has been implemented on Cadence 90nm Technology and the following results obtained for clock frequency of 1700MHz has been shown in TABLE below.

Fault Detection Approaches	Fault Coverage for Multiple Faults
GF_1 and GF_2 [15]	97%
Reconfigurable Cell Array [1]	98%
Fault Detection by Composite Fields [12]	97%
On-Line Self-Test Architecture [9]	99.99%
LUT Faults (AES Combinational Logic) [20]	88.4%
Our Implementation	100%

TABLE 2: Implementation results of XTS-AES for fault coverage

Family	Area (μm^2)
ASIC 180nm and 130nm [7]	1162489 and 542648 respectively
Our Implementation ASIC 90nm	256980

TABLE 3: Implementation results of XTS-AES for area

Technology	Throughput (Gb/s)
ASIC 180nm and 130nm [7]	27.4 and 37.3 respectively
ASIC 90nm [5]	3.7
ASIC TSMC 0.09 µ LV [5]	7
ASIC 90nm [5]	3
ASIC 90nm [5]	2-16
Our Implementation ASIC 90nm	42.5

TABLE 4: Throughput results of XTS-AES

Technology	Power Analysis (mW)
0.18 µm [11]	54 mW
0.18 µm [10]	20.35mW
0.18 µm [2]	110mW
Our Implementation	20.19853mW

TABLE 5: Low-power results of XTS-AES

From the above results, we conclude that our design takes the maximum throughput and offers 100% FC when compared to the previous methods and the reliability of the component is also high w.r.t reusability technique. The drawback of this method is it takes 3 clock cycles to reshoot the system to normal operation. The future implementation of it may be FPGA implementation of Fault Tolerant XTS-AES and image encryptions and also deriving the same for other keys namely 384 and 512 and also for XTS -AES Decryption

VI. CONCLUSION

In this paper, low power AES encryption and decryption has been designed. Parity based fault detection scheme for the low power S-box and the Inverse S-box are presented in order to find the faults in the hardware

implementation of the S-box and the Inverse S-box. Instead of using the look-up table approach for the implementation of the S-box and its parity prediction, the composite field arithmetic with logical gates is used. Simulation results show that very high error coverage for the presen ted scheme is obtained when compared to other fault detection schemes like those based on LUTs and redundant units. Also low power and low area is

achieved when compared to previous methods. An alternative lightweight design for both forward and inverse mix columns operation required also included in the AES hardware implementation. The comparisons indicate that the proposed mix-column design have less complexity than previous relevant work in gate size and no. of clock cycles.

REFERENCES

[1] Alireza Hodjat, David D. Hwang, Bocheng Lai, Kris Tiri and Ingrid Verbauwhede, “A 3.84 Gbits/s AES Crypto Coprocessor with Modes of Operation in a 0.18-µm CMOS Technology”, GLSVLSI '05 Proceedings of the 15th ACM Great Lakes symposium on VLSI,, pp.60-63, 2005.

[2] Athanasios P. Kakarountas, Epameinontas Hatzidimitriou, and Athanasios Milidonis High-throughput ASIC implementation of an encryption core for securing shared storage media, IEEE International Conference on Digital Signal Processing, pp. 1 – 5, 2011.

[3].G. Di Natale, M. Doulcier, M. L. Flottes and B. Rouzeyre, “A Reliable Architecture for Parallel Implementations of the Advanced Encryption Standard”, Springer Journals on Electronic Test, Vol. 25, pp.269-278,2009.

[4]. Epameinontas Hatzidimitriou and Athanasios P. Kakarountas, “Implementation of a P1619 Crypto-Core for Shared Storage Media”, 15th IEEE Mediterranean Electrotechnical Conference, MELECON 2010, pp.597-601, 2010.

[5]Hongge Li, Jinpeng Ding and Yongjun Pan, “Cell arra reconfigurable architecture for high-efficiency AES system”, Elsevier Journals on Microelectronics Reliability, Vol. 52, pp.2829–2836, 2012.

[6] Y.J. Huang, Y.S. Lin, K.Y. Hung and K.C. Lin, "Efficient implementation of AES IP", Circuits and Systems, APCCAS 2006- IEEE Asia Pacific Conference , pp.1418-1421. 2006.

[7] Israel Koren and C.Mani Krishna,”Fault Tolerant Systems” Morgan Kaufman Publishers, San Francisco, CA.

[8] Jin-Hao Tu and Lan-Da Van,” Power-efficient pipelined reconfigurable fixed-width Baugh-Wooley multipliers”, IEEE Transactions on Computers, Vol. 58, pp.1346 – 1355,2009.

[9] L. Liu and D. Luke, “Implementation of AES as a CMOS core,” Electrical and Computer Engineering, IEEE CCECE 2003- ,Canadian Conference , Vol. 1, pp.53-56, 2003.

[10] Mao-Yin Wang, Chih-Pin Su, Chia-Lung Horng, Cheng-Wen Wu and Chih-Tsun Huang, ”Single and Multi Core Configurable AES architectures for flexible security”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 18, pp.541 – 552, 2010

[11] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh, “Fault Detection Structures of the S-boxes and the Inverse S-boxes for the Advanced Encryption Standard”, Springer Journals on Electronic Test, Vol. 25, pp.225–245, 2009.

[12] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh," A Lightweight High-Performance Fault Detection Scheme for the Advanced Encryption Standard Using Composite Fields", IEEE Transactions on (VLSI) Systems, Vol. 19, pp 85-91, 2011.
[13] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh, "A Low-Power High-Performance Concurrent Fault Detection Approach for the Composite Field S-Box and Inverse S-Box", IEEE Transactions on Computers Vol.60, pp.1327 – 1340, 2011.
[14] Ming Li, Wenjing Lou and Kui Ren, "Data security and privacy in wireless body area networks", Wireless Communications, IEEE, Vol.17, pp.51 – 58, 2010.
[15] Mohamed Elmoghany, Mohamed Diab, Moustafa Kassem, Mustafa Khairallah, Omar El Shahat and Wael Sharkasy," FPGA Implementation of High Speed XTS-AES for Data Storage Devices" IEEE International Conference Internet Technology and Secured Transactions (ICITST) , pp.25 – 28,2011
[16] Nabihah Ahmad, Rezaul Hasan and Warsuzarina Mat Jubadi," Design of AES S-Box using combinational logic Optimization", IEEE Symposium on Industrial Electronics And Applications (ISIEA), pp.696-699, 2010.
[17] Qian Wang, Cong Wang, Kui Ren and Wenjing Lou, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, pp. 847 –859,2011.
[18] N. Sklavos and O. Koufopavlou," Architectures and VLSI Implementations of the AES-Proposal Rijndael", IEEE Transaction onComputers, Vol. 51, pp.1454 – 1459, 2002.
[19] Sophie Belloeil-Dupuis, Roselyne Chotin-Avot and Habib Mehrez,"Exploring redundant arithmetics in computer-aided design of arithmetic data paths", INTEGRATION, the VLSI journal, Vol. 46, pp.104 – 118, 2013.
[20] Uroš Legat , Anton Biasizzo and Franc Novak, "A compact AES core with on-line error-detection for FPGA applications with modest hardware resources" Elsevier Journals on Microprocessor and Microsystems, Vol. 35, pp..405–416, 2011.
[21] H.T. Vergos and D. Bakalis, "Area-time efficient multi-modulus adders and their applications", Elsevier Journals on Microprocessor and Microsystems, Vol. 36, pp. 409 – 419, 2012.
[22] Xinmiao Zhang, and Keshab K. Parhi," High-Speed VLSI Architectures for the AES Algorithm", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol.12, pp. 957 – 967, 2004.
[23] Yingtao Jiang, Abdulkarim Al-Sheraidah, Yuke Wang, Edwin Sha, and Jin-Gyun Chung, "A Novel Multiplexer-Based Low-Power Full Adder", IEEE Transactions on Circuits and Systems-II: Express Briefs, Vol. 51, pp. 345 – 348, 2004.
[24] Zhuo Hao, Sheng Zhong and Nenghai Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability", IEEE Transactions on Knowledge and Data Mining, Vol. 23, pp.1432 –1437, 2011.