Sub Pipelined Architecture for Self-Test Techniques of Crypto Devices Based on AES With High Throughput

A.Sriram
Department of Electronics and Communication Engineering
SNS College of Engineering, Coimbatore, Tamilnadu, India

G.Yuvaraj
Department of Electronics and Communication Engineering
SNS College of Engineering, Coimbatore, Tamilnadu, India

Abstract- Testing of the equipment is very essential before being put into service. The testing has to be done by the latest technique. This paper describes a generic built-in self-test strategy for crypto devices with sub pipelining architecture by implementing symmetric encryption algorithms. Taking advantage of the inner iterative structures of crypto-cores, test facilities are easily set-up for self-test of the crypto-cores, built-in pseudorandom test generation. Main advantages of the proposed test implementation are high throughput and no visible scan chain, this testing provides crypto cores with 100% fault coverage with a notable speed has been achieved in the range of 3.22 Gbps for 128 bit AES algorithm.

Keywords – Digital circuit testing, security, self-testing, AES sub pipelining, VHDL

I. INTRODUCTION

The failure analysis of an integrated circuit is one of the most important processes by which we continuously improve the reliability of the electronics that we use every day. IC failure analysis labs are places where defective chips are sent so we can find out what went wrong and incorporate our learnings right into the manufacturing itself so that we can prevent the same mistake from happening again. This paper aims at providing efficient test solutions for possible physical failures on the electronic device implementing the cryptographic algorithm with a maximum speed of 3.22 Gbps. One approach for providing test solutions at different stages of an IC life cycle with high speed consists in including built-in self-test (BIST) resources with sub pipelining into the Circuit under test (CUT).BIST does not provide full controllability and observability of the internal storage elements from the IC interface, namely the scan-in/scan-out pins. Not only the IC testing by itself but also which generates the pattern to test other external IC too. This major difference with the external testing strategy makes the scan based attacks not usable and thus avoiding the implementation of related countermeasures .so that BIST must be implemented at low cost and which should test the device with high speed with maximum efficiency of fault coverage (FC).Let us discuss this in detail.

II. EXISTING SYSTEM

The existing system for testing the devices with pipelined architecture of high speed is 1.11Gbps ie.Different approaches like Circular BIST with State Skipping, Deterministic Circular Self-test Path, Scan-based side-channel attack on dedicated hardware implementations on data encryption standard, secure scan: A design-for-test architecture for crypto chips, Were introduced without pipeline architecture. Later the AES algorithm was introduced with pipelining for high throughput which operates at the speed of 1.11 Gbps for 128 bits.

III. AES ALGORITHM

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text and decrypting the cipher text converts the data back into its original form, called plaintext. A symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The algorithm may be used with

the three different key lengths and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256". This paper uses 128 bit AES algorithm with sub pipelined architecture to increase the speed the operation in self-testing of crypto devices.

IV. PROPOSED SYSTEM

The proposed system uses sub pipelining architecture in between four stages of AES algorithm sub bites, mix column, shift rows and add round key.

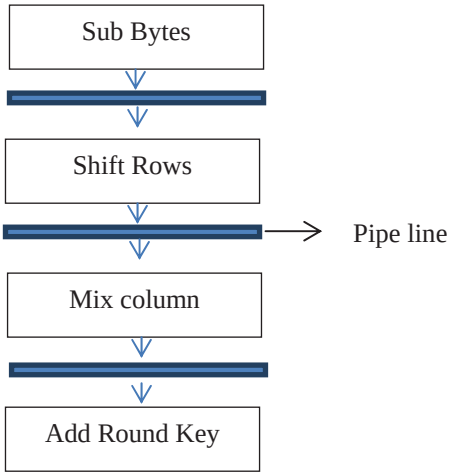

Figure 1. The basic block of the AES core

In the Figure 1 a 128 bit pipelining register is introduced in between each blocks which contains four Separated blocks, SubBytes, ShiftRows, MixColumns and AddRoundKey. This full block is repeated ten times in the AES core to get the whole result. In manufacturing of IC the IC should be tested in various stages and each stage would be tested with the pre generated pattern of good IC's. Normally the crypto devices are used for sending the data with more secure. If the same devices can be used to check other devices fault or good then we can avoid the fault checking with different devices. This paper proposed of three test modes (SELF_TEST, TPG, ORA) in terms of randomness, aliasing, and cost of implementation and speed are discussed and supported by experimental results.

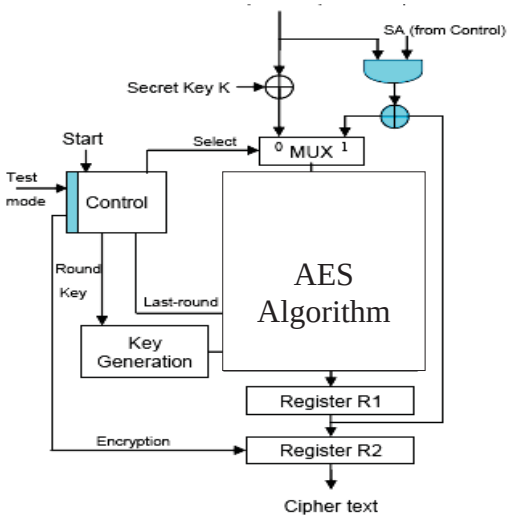

Figure 2. Implementation of crypto core

Initially the XOR operation is done between Key and Plaintext then the plaintext block is looped around the Round module several times (10 for AES). As sub pipeline is introduced in each stage for each round the through put can be very fast. In SELF_TEST mode of operation the SA signal must be 0 so that the XOR operation is skipped. An initial message is encrypted and the process is repeated 10 times.

The final data is stored into R-out register for the comparison with expected correct value. Now sub-pipeline structure increases the maximum frequency significantly and the average delay in between blocks should be controlled by sub-pipeline to reduce the maximum delay to average latency time, the frequency increased from 35.411 MHz to 103.061MHz by inserting four registers so that comparing with a design without sub-pipeline, the sub-pipeline design improves the performance.

During the Test pattern generation mode the SA signal must be 1 and select must 0. When it is set the device generates the pattern for the particular circuit which is to be tested. In ORA mode, the output of CUT (Circuit Under Test) is fed back as an input to the device. In this time SA and Select are set to 1, so that an XOR operation is performed between one response of the CUT and the result of the previous round in the crypto-core. The final signature obtained after compaction of all the test responses is loaded into R-out register.

V.SUBPIPELINING

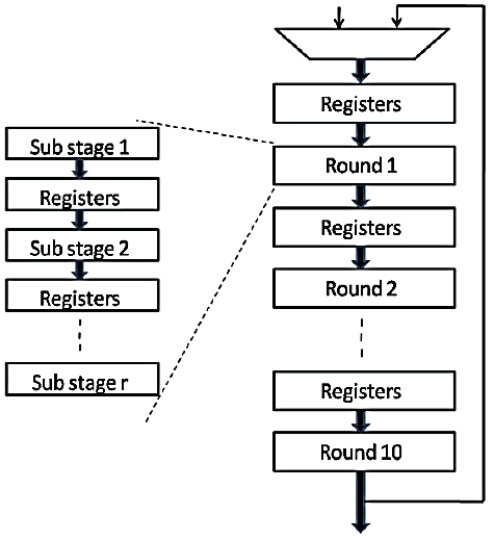

Figure 3. Implementation of Sub pipelining

In order to increase the speed of operation in self- test technics the registers are inserted both between and inside each round of each stage. So that the maximum speed and better throughput can be obtained. In the sub pipelining method the plain text is received through registers at all clock cycles. At each clock cycle data is shifted to next stage and final output is appeared only after the end of ((10*r)+10) the clock cycle. Here 'r' represents number of sub pipeline stages. The biggest advantage of this sub pipelining is that the second output can be obtained at once in sub sequenced clock cycle. In order to complete 10 rounds the AES algorithm takes 1200 ns without pipelining but when the sun pipelining is introduced the AES algorithm takes 21 ns to complete 10 rounds thus increases the speed of self- testing and test pattern generation and output response analysis operations along with encryption with high throughput.

VI. SELF-TEST MODE

When the crypto device is being manufactured for the particular operation then the device is needed to be tested after the manufacturing so that the device will be known as fault or correct. This can be done by the external device for testing it. If the device can test itself with more speed then identifying the number fault and correct devices after manufacturing will be done so fast which increases more number of devices to be manufactured without failure. The presence of a fault modifies the AES round output and thus the next test pattern (circular scheme). This is taken into account in our experiments in which we injected every single stuck-at fault, fault simulated the circuit, An S-box

needs *k* deterministic patterns to be fully tested and it receives one random pattern every clock cycle. Since the other parts have lower complexity than the S-boxes, it can be expected that they will be fully tested by the time the S-boxes received a sufficient number of test patterns.

VII. Test Pattern Generation Mode

When the external device is to be tested then the corresponding circuit will be taken as CUT (Circuit Under test) and the test pattern will be generated for the particular circuit which investigates how good the sequences are compared to standard generated sequences for random testing.

VIII. Output Response Analyser Mode

In the Output Response Analysis mode the generated test pattern will be compared with the standard pattern. If both patterns are equal then the device is fault free else the device is having fault.

IX. Performance Analysis

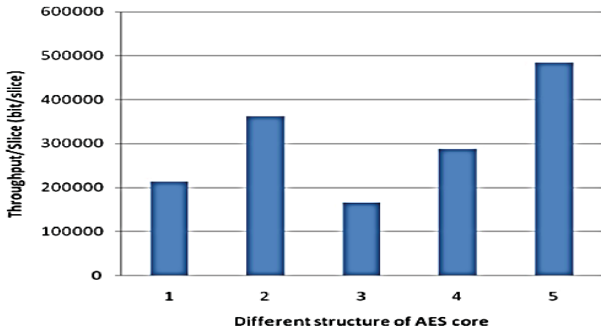

Figure 4. Comparison of Different structure of AES core with throughput

In the Figure 4 y-axis determines the “Throughput /Slices” in each structure and it is obvious that the fifth one which is the sub-pipelined structure, has the highest rate of “Throughput/Slices”.

Table -1 The total statistics of the AES core

	Combination of different method applied	Slices	Throughput
1.	Composite field SubBytes for both Key Expansion and SubBytes	5207	1.11Gbits
2.	Composite field SubBytes for KeyExpansion and look up table for SubBytes	6385	2.32Gbits
3.	Composite field for SubBytes and look up table for Key Expansion	6659	1.11Gbits
4.	Look up table for both Key Expansion and SubBytes	7606	2.19Gbits
5.	Sub-pipelined SubBytes	6605	3.22Gbits

X.RESULTS AND DISCUSSION

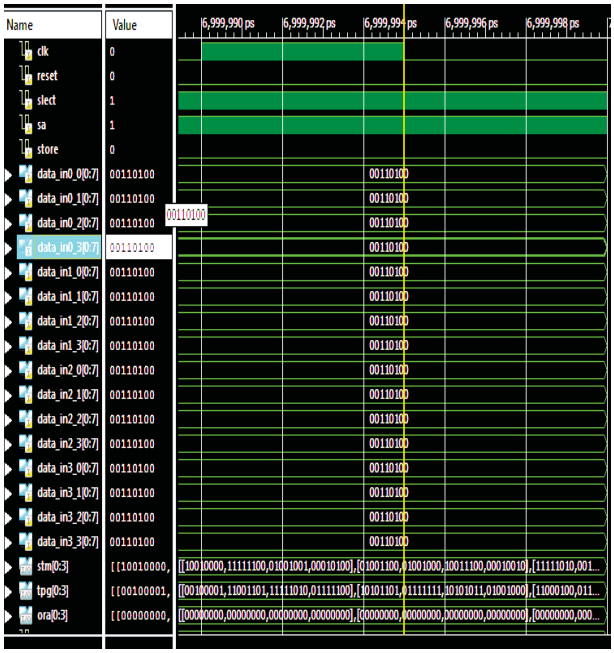

Figure 5: Output of STM, TPG and ORA mode

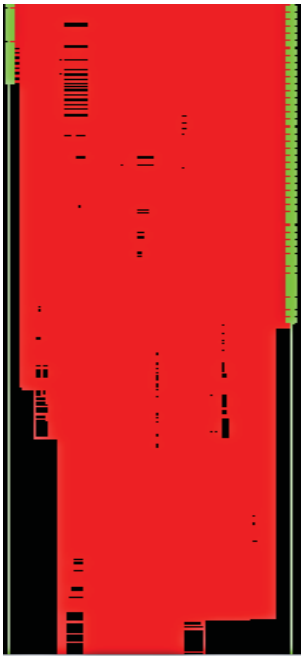

Figure 6. Schematic view of AES Crypto core

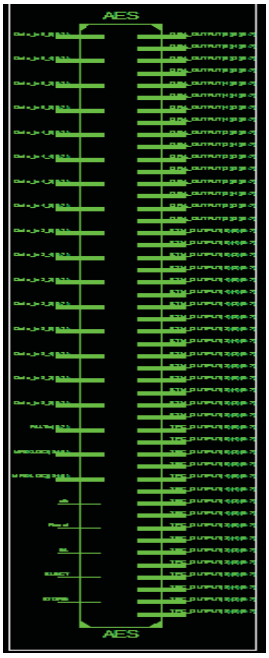

Figure 7. RTL view of AES Crypto core

This paper was successfully completed with the implementation of Sub pipelined architecture for self-test technicsfor crypto devices with high throughput based on AES algorithm. By using VHDL code the crypto core is implemented with different sub modules. This implementation will be useful in wireless security and testing of other devices to check fault or correct and the speed of transmission

XI. APPLICATIONS

These crypto core devices can be used in

- Smart Cards
- RFID.
- ATM networks.
- Image encryption

For Secure Storage

- Confidential Cooperate Documents
- Government Documents
- FBI Files
- Personal Storage Devices
- Person Information Protection

XII. CONCLUSION

The transmission of data for the communications with more secure the cryptography device is used. If the same device is used to check the fault in other devices and in itself with more speed then the same deceive will be used for multiple purpose like high speed transmission, preventing the fault IC to be manufactured again. As proposed sub

pipelined architecture for self-test technique whose code is to feed the core with its output and the device can be run for a certain number of encryption to compare the output with pre computed output with the speed of 3.22Gbps and maximum of 100 % fault coverage is achieved.

XIII. ACKNOWLEDGEMENT

This work was supported in part by their institution to bring up the ideas and develop the project. The authors would like to thank their Parents, Relatives – Mr.Veluchamy and Mrs.Latha Veluchamy, Staffs, Principal and the administration and also like to thank the anonymous reviewers for their constructive comments which greatly improved the quality of this work.

REFERENCES

[1] Tanzilur Rahman, Shengyi Pan, Qi Zhang "Design of a High Throughput 128-bit AES " proceedings of the International Multiconferene of engineers and computer scientists 2010 Vol II IMECS 2012,March 17-19,2010,Hong Kong

[2] Giorgio Di Natale, Marion Doulcier, Marie-Lise Flottes, and Bruno Rouzeyre "Self-Test Techniques for Crypto-Devices " IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 18, NO. 2, FEBRUARY 2010

[3] M.Pitchaiah, Philemon Daniel, Praveen " Implementation of Advanced Encryption Standard Algorithm" International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518

[4] Subashri T, Arunachalam R, Gokul Vinoth Kumar B, Vaidehi V Department of Electronics, MIT Campus, Anna University, Chennai-44 "Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory" International journal of VLSI design & Communication Systems (VLSICS) Vol.1, No.4, December 2010

[5] M. Doulcier, M.-L.Flottes, and B. Rouzeyre, "AES-based BIST: Self-test, test pattern generation and signature analysis," in Proc. 4th IEEE Int. Symp. Electron.Des., Test Appl. (DELTA), 2008, pp. 314–321.

[6] D. Hely, F. Bancel, M.-L. Flottes, and B. Rouzeyre, "Securing scan control in crypto chips," J. Electron. Test.: Theory Appl., vol. 23, no. 5, pp. 457–464, Oct. 2007.

[7] J. Elbirt, W. Yip, B. Chetwynd and C. Paar, "An FPGA Implementation and Performance evaluation of the AES Block Cipher Candidate Algorithm Finalist, "The third AES Conference (AES3), New York, Apr. 2000. Available at http://csrc.nist.gov /encryption/aes/round2/conf3/aes3papers.html.

[8] J. Elbirt, W. Yip, B. Chetwynd and C. Paar, "An FPGA Implementation and Performance evaluation of the AES Block Cipher Candidate Algorithm Finalist" IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 9, NO. 4, AUGUST 2001.

[9] X. Zhang and K. K. Parhi, "Implementation Approaches for the Advanced Encryption Standard Algorithm," IEEE Circuits and Systems Magazine, vol.2, Issue.4, pp. 24-46, Fourth Quarter 2002.

[10] K. Gaj and P. Chodowiec, "Hardware performance of the AES finalists survey and analysis of results." [Online]. Available citeseer.ist.psu.edu/460345.html

[11] National Institute of Standards and Technology, Specification for the Advanced Encryption Standard (AES). FIPS PUB 197, available at http://csrc.nist.gov, 2001.

[12] Kris Gaj, Pawel Chodowiec, "Comparison of the hardware performance of the AES candidates using reconfigurable hardware", International conference on Advanced encryption standard candidate conference, April 13, 2000.

[13] John Kelsey, Bruce schenier, "MARS attacks! Preliminary cryptanalysis of reduced round MARS variants", Third international conference on advanced encryption standard candidate conference, 2000.

[14] Lan Harvey, "The effects of multiple algorithms in the advanced encryption standard", International Conference on advanced encryption conference, 2000.

[15] FIPS (Federal information processing standards), "Advanced Encryption Standard", issued by NIST, November 26, 2001.

[16] D.Richard Kuhn, Thomas J. Walsh, Steffen Fries,"Security Considerations For Voice Over IP Systems", NIST Special Publication, January 2005.