An Efficient Self Testing Cryptographic Systems For Low Power Applications

M.K KISHORE [1], P.YAMINI DURGA[2] K.BABURAO[3], Mrs.K.NITYA[4]
[2](USHARAMA COLLEGE OF ENGINEERING AND TECHNOLOGY, Telaprolu, M.Tech Student)
[3](USHARAMA COLLEGE OF ENGINEERING AND TECHNOLOGY, Telaprolu, Assoc.prof)
[1,4](USHARAMA COLLEGE OF ENGINEERING AND TECHNOLOGY, Telaprolu, Asst.prof)

ABSTRACT : Today security is very important parameter to communicate between other peoples. Now a days we observe sometimes hacking the information like passwords, bank account numbers etc. so, we provide security between end to end process. This security can be achieved by using of testing methods. The traditional testing methods are good at detects only random faults, but they do not good to secure all types of attacks. In this paper design an Logic Built In Self Test (LBIST) to detect the faults. Here, we use feedback shift register based cryptographic system. Cryptographic systems are used to secure the confidential information between end to end communication by using Advanced Encryption Standard (AES Crypto Core) algorithm. Linear feedback shift register is used to generate all the possible test patterns and patterns are verified by LBIST. This project can be extended to replace the linear feedback shift register by Bit Swapping LFSR(BS LFSR). In BS LFSR, uses Multiplexer(MUX) circuit to generate the test patterns simply by swap the bits depends on selection line. This BS LFSR technique decreases power consumption by 25 to 50%.

***Key Words*:** LBIST, LFSR, Crypto device, AES, symmetric key, BS LFSR

I.INTRODUCTION

Now a day's most of the users using wireless communication technology and in this technology they are both advantages and disadvantages. The main disadvantage is hacking the information from the others. In our project, use Advanced Encryption Standard(AES) technique to protect the information from the hackers.

Over all of the techniques power consumption is a major problem in chip designing that contains a very large number of transistors. High power consumption causes circuit damage and reduces the life time of the product.

Several techniques have been developed to reduce the power consumption. One of the direct technique to reduce average power consumption is by running the test at a slower frequency than that in normal mode. This technique fails the reducing peak power consumption because it is independent of clock frequency and also increases the time.

Another technique is used to reduce the power consumption in LFSR based BIST technique is replaced the normal LFSR with bit swapping LFSR. By using bit swapping LFSR technique which reduces the number of transitions that leads to decreases power and time.

Feedback Shift Register (FSR) based cryptographic systems are the fastest and the efficient cryptographic systems for hardware applications.

Many cryptographic algorithms were proposed, such as the Data Encryption Standard (DES), the Elliptic Curve Cryptography (ECC), the Advanced Encryption Standard (AES). Here the implementation of AES algorithm with LBIST is presented to increase the data transfer speed and security. The power optimization for the circuit is attained through bit swapping technique used in the circuit results in less time.

II.PROPOSED WORK

In this paper the design of Logic Built-In Self-Test (LBIST) for Linear Feedback Shift Register (LFSR) based cryptographic system(AES crypto core) by using bit swapping LFSR is implemented. The block diagram of the presented method is shown in figure 1.

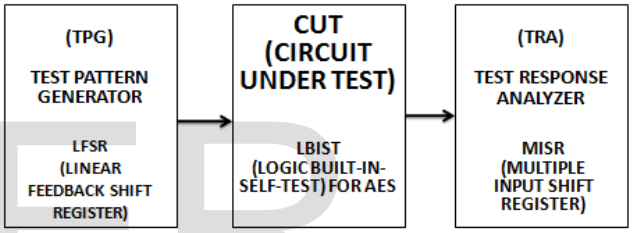

Figure 1: Block diagram of presented method

2.1 LFSR

LFSR is used to generate all the possible test patterns depends on the initial input sequence and tap connection. In this paper design an 128 bit LFSR to generate all the 128 bit input combinations. LFSR is a linear feedback shift register whose input bit is a linear function of previous function that contains the signal through the register from one bit to the next most significant bit when the clock is applied.

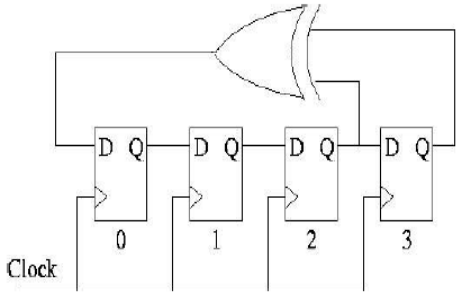

Figure 2: Diagram of Test Pattern generator using LFSR

It can be made simple by performing exclusive-OR gate operation on the outputs of two or more of the flip flops. The output of exclusive-OR gate is fed back to the input of the one of the flip flop. The main drawback of LFSR is which generates pseudo random patterns that leads to high power

dissipation and high switching activities in Circuit Under Test(CUT).

A maximal-length LFSR produces the maximum number of possible patterns and has a pattern count equal to $2^n - 1$, where n is the number of register elements in the LFSR.

2.2 AES CRYPTO CORE

The AES crypto core algorithm mainly consists of encryption process, key generation and decryption processes that are explained in the following subsections.

2.2.1AES ENCRYPTION

Encryption is the process of converting information from one from to another form. The original message in the encryption process is called the plain text while the scrambled data i.e converting data, after the encryption is called the cipher text. The plain text can be recovered from the cipher text with a decryption process using a key. The algorithm that can perform encryption and decryption is called a cipher.

The AES encryption algorithm converts plain text into cipher text by using an encryption key and consists of several rounds of encryption operation. The AES converts a block of 128 bit plain text into a 128 bit cipher text with the help of a 128 bit secret key. After a first XOR operation between key and the plaintext, the algorithm consists in several rounds: 10, 12 or 14 rounds according to the key length 128, 192 or 256 bits. Every round except the last one is composed of four operations. 1.Sub bytes 2.Shift rows 3.Mix columns 4. Add round key The structure of AES encryption is shown in figure 3.

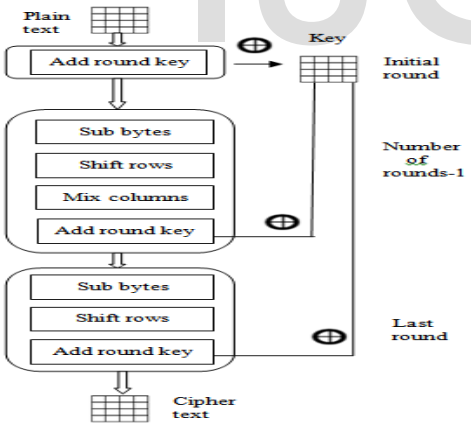

Figure 3: AES encryption structure

2.2.2 AES KEY GENERATION:

The key generation process is used to describe the operation of generating all round keys from the original input key. The initial round key will be obtained from the original key in case of encryption and the last group of the generated expansion keys uses in case of decryption[6]. The Round CONstant(RCON) value changes for each individual round. The AES key generation structure is shown in figure 4.

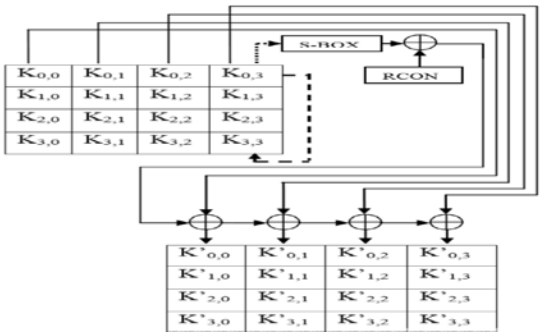

Figure 4: AES key generation structure

2.2.3 AES DECRYPTION

AES decryption is inverse operation of the encryption. AES decryption process converts cipher text into plain text(original message). As shown in figure 5, the state vector goes through mathematical functions and the resultant is the plain text which was given as input to the AES encryption.

The process is nearly identical to the encryption counterpart, except that the rotation is towards right and the Inverse S-Box is used for substitution and for the Inverse mix columns operation, the difference is the multiplication matrix, which is inverse of the matrix mentioned in encryption. In the last round, Inverse mix column transformation is not done and the output of Inverse add round key of last stage is taken as the decrypted data. The structure of AES decryption is shown in figure 5.

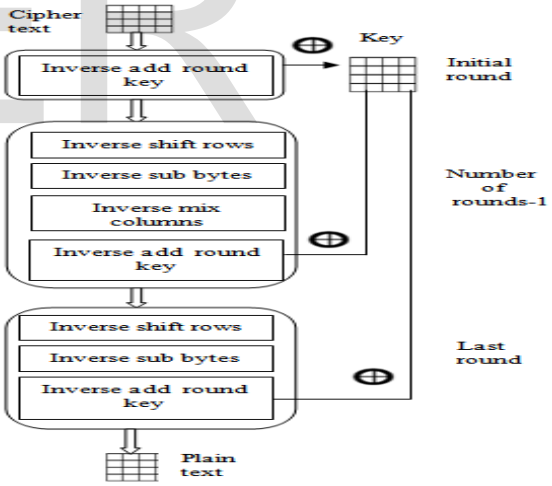

Figure 5: AES decryption structure

2.3 LBIST

BIST is an better solution for testing problems and detects the faults. Testing is faster and efficient because circuit is built into hardware. It consists of several blocks.

1.Circuit Under Test (CUT): It can be combinational or sequential circuit to be tested.

2.Test Pattern Generator (TPG): It generates test patterns for CUT.

3.Test controller: It controls the execution of the test. If the signal from the test controller is 0, then the BIST is said to be in test mode otherwise it is said to be in normal mode.

4.ROM: It stores the signature which is compared with CUT output.

5.Response Analyzer: It compares the test output with the stored signature. If the output matches then the CUT is non faulty otherwise it is faulty circuit. The block diagram of basic BIST circuit is shown in below figure.

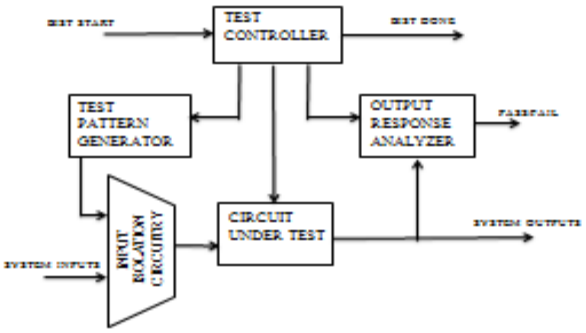

Figure 6: BIST basic block diagram

2.4 BIT SWAPPING LFSR:

The presented method can be extended by using bit swapping LFSR .Bit Swapping LFSR is a modified type of conventional LFSR which generate test patterns with less transitions. It reduces the average power dissipated by CUT. The power consumption of CUT depends on internal reduction of switching. BS LFSR reduces average and instantaneous switching activity. Power consumption can be reduced by several techniques. Direct techniques are not efficient for peak power reduction and increases the test time. BS LFSR reduces average and peak power dissipated by CUT, compared to other techniques. The general architecture of bit swapping LFSR is shown in below figure 7.

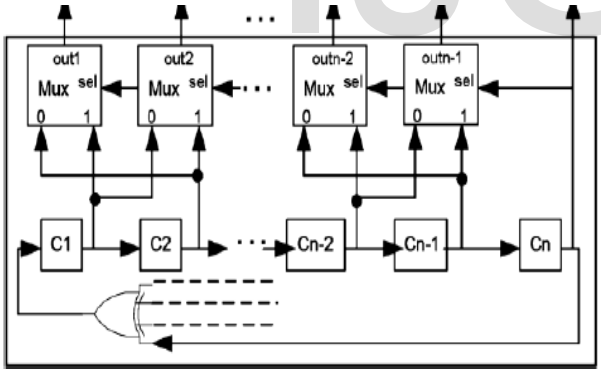

Figure 7: General architecture of Bit Swapping LFSR

Consider an n-bit length of LFSR. One of its outputs (last bit i.e. n_{th} bit) to be a selection line that will swap two neighboring bits. If the value of selection line is set to 0 for swapping and n is made odd (bit n=0), then bit 1 will be swapped with bit 2, bit 3 is swapped with bit 4…..bit n-2 with bit n-1. If n is made even (bit n=0), then bit will be swapped with bit 2, bit 3 with bit 4…bit n-3 with bit n-2. If n=1, then no swapping operation is performed. The number of transitions is saved by using swapping arrangement. This BS LFSR technique decreases power consumption by 25 to 50%.

III RESULTS

This circuit is implemented by using VHDL as the hardware description language. The software used for this work is Xilinx ISE 13.1.

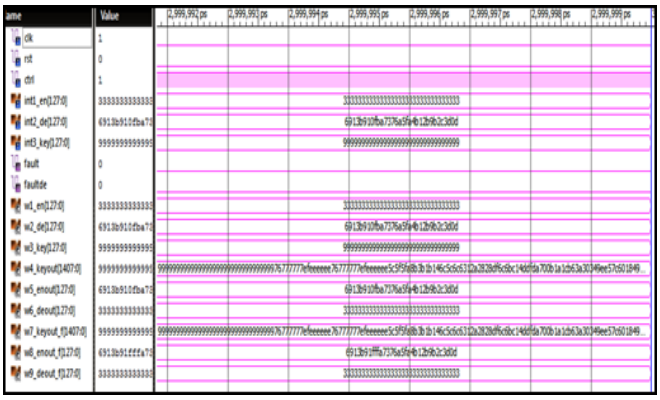

Figure 8: Simulation results of LBIST mode

In figure 8 the simulation results of Built-In Self-Test are shown when there is no fault i.e comparison between the output of theoretical circuit and practical circuit and performs the self test and indicates as 1 if fault is present or else indicates as 0 if there is no fault. As the practical circuit is fault free, the fault en(indication of fault at encryption side) and fault de(indication of fault at decryption side) are both 0 indicating that the circuit is fault free.

POWER ANALYSIS

Power Analysis is done using Xilinx Power Analyzer. Power is reduced by using bit swapping LFSR technique. Without using bit swapping LFSR the power consumption for the circuit is 0.174 W as shown in figure 9 and with using bit swapping LFSR the power consumption for the circuit is 0.158W as shown in figure 10.

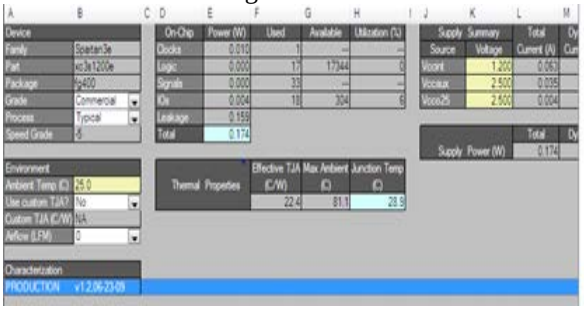

Figure 9: Power report without using bit swapping LFSR technique.

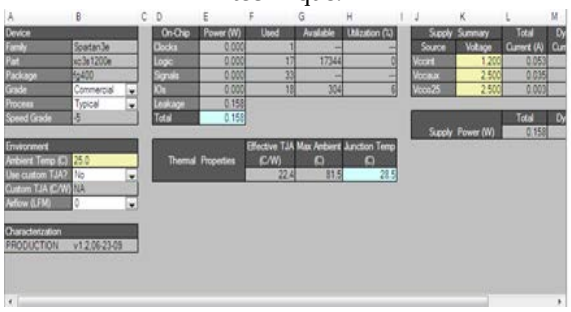

Figure 10: Power report using bit swapping LFSR Technique.

IV CONCLUSION

LFSR are widely used in digital circuit to generate test patterns and to compress the output sequences of the CUT. This paper presented the design of a Bit Swapping LFSR using VHDL which has the characteristics of low power consumption and suitable in processing environment where uniform distribution random numbers are required. Results show that Bit-swapping LFSR reduce transition states. Comparison between implemented BIST schemes by normal LFSR and Bit-swapping LFSR show that Bit-swapping LFSR can easily replace the normal LFSR for better result. The experimental results on Xilinx tool shows the effectiveness of proposed method and 25% reductions in dynamic power with respect to the conventional LFSR

V ACKNOWLEDGMENT

The authors would like to thanks Mr.M.K.Kishore for his contributions to Section I, Mr.K.Baburao for his contributions to Section III, Mrs.K.Nithya for his contributions to Section IV. The authors would also like to thank Dr.V.Rajesh for his software radio implementation contributions to the research.

VI REFERENCES

[1] Lubna Naimand Tarana A. Chandel," Implementation of modified test pattern generator for BIST application" in IJAET March 2014.
[2] V.Kirthi, Dr. G. Mamatha Samson," Design of low power test pattern generator" in IOSR Journal of VLSI and Signal Processing September 2014.
[3] K. Supriya1, B. Rekha, "Implementation of Low Power Test Pattern Generator Using LFSR" in International Journal of Science and Research (IJSR), August 2013.
[4] Md. Fokhrul Islam, M. A. Mohd. Ali, BurhanuddinYeopMajlis, "FPGA Implementation of an LFSR based Pseudorandom Pattern Generator for MEMS Testing", in International Journal of Computer Applications, August 2013.
[5] SeagmoonWang „ " A BIST TGP for low power dissipation and high fault coverage", IEE transaction on very large scale integration (VLSI) system, vol.15, no.7 july 2007.
[6] Poornima M, "Implementation of multiplier using vedic algorithm", International journal of innovative technol--ogy& exploring engineering (IJITEE) Vol-2,issue-6,May 2013.
[7] Ajit Kumar Mohanty, BiswanathPratapSahu, ChandanPatnaik, S. S. Mahato."Low Power Test Pattern Generator for System on Chip Architecture", International Conference on Computing, Communication and Sensor Network.
[8] P.H. Bardell and W.H. McAnney, "Pseudorandom arrays for built-in test", IEEE Transactions on Computers.

VII BIOGRAPHY

Mr.M.K.Kishore,workingas Asst.professor of ECE department in USHARAMA college of engineering and technology. M.Tech degree DECS (DigitalElectronics& Communication Systems) from Gudlavalleru Engineering College Affiliated to JNTUK Gudlavalleru, in 2010, B.Tech degree in Electronics and Communication Engineering from Nova College of Engineering and Technology Affiliated to JNTUH Jangareddygudem in 2008. He has a total teaching experience of 5 years. His research areas include Embedded System

Ms. P.Yamini Durga is pursuing her M.Tech degree in VLSI& EMBEDDED SYSTEMS from, Usharama College of Engineering and technology, Telaprolu Affiliated to JNTUK B.Tech from Electronics & Communication Engineering from Sri Sunflower College of Engineering & technology Affiliated to JNTUK, chalapalli in 2012.

Mr.K.Baburao, working as associate professor of ECE department in USHARAMA college of engineering and technology. M.Tech in DECS (DigitalElectronics& Communication Systems)from GEC College Affiliated to JNTUK Passed out in 2007.B.Tech in ECE, from KLC Engineering College Affiliated to NAGARJUNA UNIVERSITY Passed out in 2003. He has a total teaching experience of 11 years His research areas include Embedded System.

Mrs. K.Nitya workingas Asst.professor of ECE department in USHARAMA college of engineering and technology. M.Tech degree in VLSI& EMBEDDED SYSTEMS from, Usharama College of Engineering and technology, Telaprolu Affiliated to JNTUK B.Tech from Electronics & Instrumentation Engineering from NOVA College of Engineering & technology Affiliated to JNTUH, Jangareddygudem in 2007. Her research interest includes Embedded Systems.