ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Parallel CRC Generation with Secured LBIST

N.Prasad
M.Tech,
Department of ECE,
Bhimavaram Institute of Engineering Technology,
Pennada, Bhimavaram, Andhra Pradesh, India.

P.V.V.Rajesh
Assistant Professor,
Department of ECE,
Bhimavaram Institute of Engineering Technology,
Pennada, Bhimavaram, Andhra Pradesh, India.

ABSTRACT:

Cryptography systems are Increases for efficient and secure transmission in different applications. Whenever the requirements and applications are gains the architecture and complexity there by causes the occurrence of the different errors and faults. In present advance systems we cannot tolerate even the small faults and failures for that we rely on the traditional faults detection mechanisms like BIST and others. These are good for the detecting the traditional faults but they fail to detect the untraditional faults like Trojans.

Even the small normal Trojans also cannot be detected by the traditional testing mechanism. The flops or memory testing necessitates for proper operation for the present high end throughput designs in order to achieve the appropriate testing rather than the scan chains for all untraditional faults that occurred in smaller designs. A novel design method can be proposed in this paper for the faults detections which ids described above. Proposed concept based designed for the parallel CRC computation circuit is designed using the verilog, simulated using the modelsim and synthesized using the Xilinx

I.INTRODUCTION:

Cryptography systems are increasing in different applications for the secure and efficient data transmission between source and destination. There by the possibility of faults also increases. By using the traditional testing mechanisms are well efficient for testing the traditional faults but they fails for the untraditional faults like Trojans. Because the data in not properly encrypted there may be problem can be occurred at the decryption also, there by causes the improper communication and also data loss. This we cannot accept by the present improved designs. They are several attempts were made for the proper testing mechanism by adapting the novel test patterns and other methods.

But they may fails for even for detecting the small Trojan effects. those are well suited for the detection of the normal traditional faults and failures. In general any Logical BIST architectures are designed by the automatic test pattern generation along with response analyzer that can associate with the scan chains. In general with scan chains the delay will be introduces with the operation with the test mode. The time taken to operate in the test mode is much greater than the normal operation mode. And more over the traditional test pattern generation based LBISTs are not suitable for the advanced designs because they cannot detects the simple Trojans.

For the better architecture based on the LBIST can be achieved by the proposed method with novel approach for the testing of the memories and flops. In present systems CRC calculations can be efficient for all cryptography systems but serial calculations may take several clock cycles this gives the time taken process for the calculation can as well as the transmissions. For the improved parallel calculations can be carried out by the parallel CRC architecture. This paper distributed as the Introduction at session I and the parallel CRC calculation circuit and followed by the proposed novel LBIST design, next session can be results and discussions and followed by the conclusion and references.

II CRC ARCHITECTURE:

In general calculation of CRC can be through the liner feedback shift register (LFSR) it performs binary division with the selected polynomial. It can be performed by the successive shifting and subtractions. As we know the addition, subtractions and multiplication for general modulo 2 arithmetic are equivalent to the bitwise XORs and AND planes respectively. The basic diagram of the serial LFSR can be shown in below figure. In the above fig serial data input is ‘d’, present state generated CRC is X, X’ is next state and generator polynomial is P.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

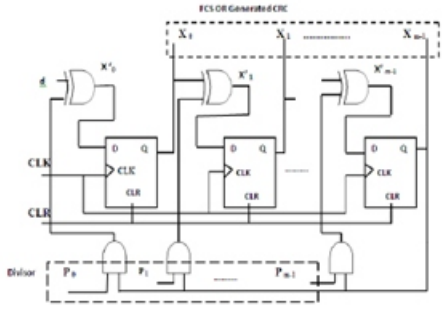


Figure1. Basic LFSR Architecture

In the above fig serial data input is 'd', present state generated CRC is X, X' is next state and generator polynomial is P.

$$X_0' = (P_0 \otimes X_{m-1}) \oplus d \quad (1)$$

$$X_i' = (P_0 \otimes X_{m-1}) \oplus X_{i-1}$$

The generator polynomial for CRC-32 is as follows

G(x) = x32 + x26 + x23 + x22 + x16 + x12 + x11 +x10 +x8 + x7 + x5 + x4 + x2 + x1 + x0;

We can extract the coefficients of G(x) and represent it in binary form as

P = {p32, p31,……, p0}

P = {10000010011000001000111010110111}

The problem that is associated with the serial calculation of the CRC using the LFSR is the operation time in general it requires the (i+j) clock cycles where 'i' is the number of the data bits and the 'j' is the polynomial bits. It may take the negligible time consumption.In order to overcome the problems that are occurred in calculating the CRC in serial mode we prefer the parallel mode. Even though the parallel operation circuit can be increased in the area and power we give more priority for the operation time.

A. Algorithm for F matrix based parallel architecture:

For Parallel CRC generation architecture F-matrix based design is the more efficient and sophisticated method the basic diagram for the parallel CRC calculation based on f-matrix can be shown below

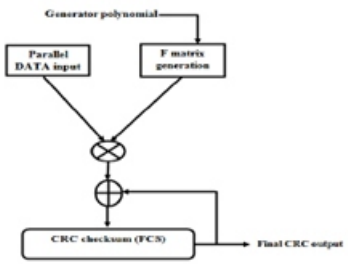
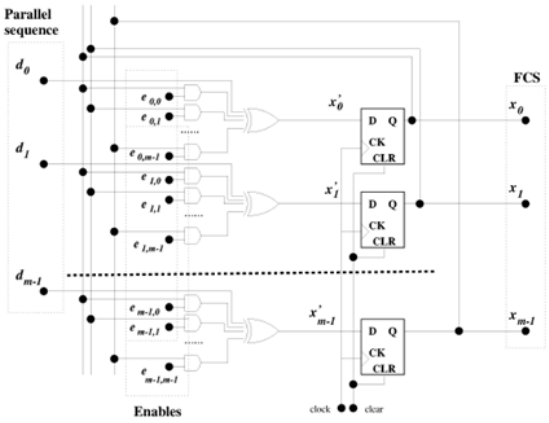


Figure2: Algorithms for F matrix based architecture

Parallel data input and each element of F matrix, which is generated from given generator polynomial is anded, result of that will xoring with present state of CRC check-sum. The final result generated after (k+ m) /w cycle.

B.F Matrix Generation:

$$F = \begin{bmatrix} P_{m-1} & 1 & 0 & 0 & 0 \\ P_{m-2} & 0 & 1 & 0 & 0 \\ P_{m-3} & 0 & 0 & 1 & 0 \\ P_{m-4} & 0 & 0 & 0 & 1 \\ .. & .. & .. & .. & .. \\ P_0 & 0 & 0 & 0 & 0 \end{bmatrix}$$



Figere3. Parallel CRC architecture

Below equations shows the F-matrix calculation examples with w=m=4

$$F = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad (3)$$

Here w=m=4, for that Fw matrix calculated as follow.

$$F^4 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad (4)$$

F matrix is generated from generator polynomial as per above Where, {p0……pm-1} is generator polynomial. For example, the generator polynomial for CRC4 is {1, 0, 0, 1, 1} and w bits are parallel processed.

C. Advanced Parallel Architecture:

The parallel architecture that able to process the bits where the w ≤ m, w ≥ m and w=m From the above architecture the e0 to ei-1

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

are the calculated F-matrix based on the parallel bit processing i.e. if we are processing the 24 parallel bits then we need to calculate the F-24 matrix. For each and gate matrix row and the previous data X given as the input and that is XORed with the present data input 'd' will be give to the flop for storing the present output for the next calculation. The architecture of parallel CRC calculation is shown in figure4.

III. PROPOSED TEST SETUP FOR THE PARALLEL CRC ARCHITECTURE:

In parallel processing CRC architecture internally consists of Flops in the design as we discussed in previous session scan chains are not the ideal approach for the testing. So we made several changes for the better test setup design.
A) Logical built in self test This is one of the designs for testability (DFT) mechanism that can able to test the circuit at the run time. The advance design feature that has capable of tasting using the built-in test setup that able to increase the testing standards and also the testing time.

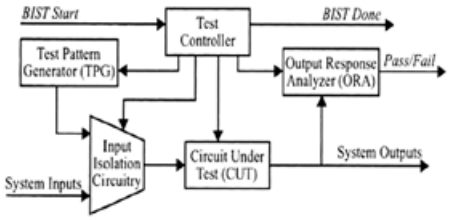


Figure4. BIST Basic block diagram.

The basic BIST requires the elements like pest pattern generator for proving the test input patterns, test controller used for entire test control and response analyzer used for the analysis of outputs of form the CUT and tells whether test is pass or fail.

B) Proposed Parallel Architectu:

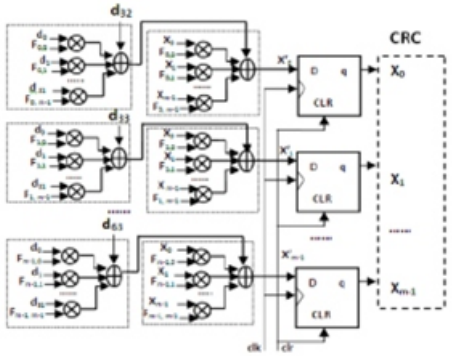


Figure.5: The architecture of 64 bits processing

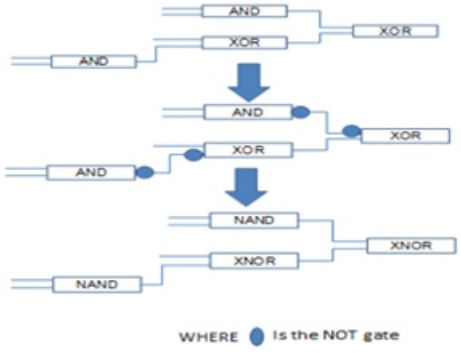


Figure6: replacing the architecture

In the CRC-32, for 64 bit processing it has 2048 AND gates. By replacing the AND with NAND, it is free of area by 2 CMOS transistor per gate. It uses 2048 AND gates and so by replacement with NAND, 2048*2=4096 CMOS transistors are reduced. And it is 33% area efficient architecture.

B) Proposed flop design:

Unlike scan chains each flop can be multiplexed with the input data and the test data. The selection of data can be done through the model selection through the test control setup. And for the verification also we take control enable for connecting the output to the test response analyzer or operation output.

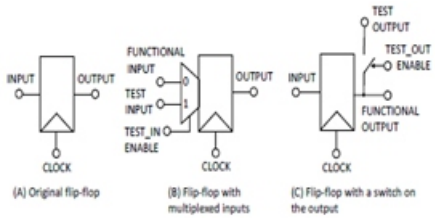


Figure.7: Modifications in flip-flops design to support LBIST

The above parallel CRC calculation architecture can be designed by using the above flop design. By this we can efficiently detect the faults and failures very easily.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

IV RESULTS AND DISCUSSIONS:

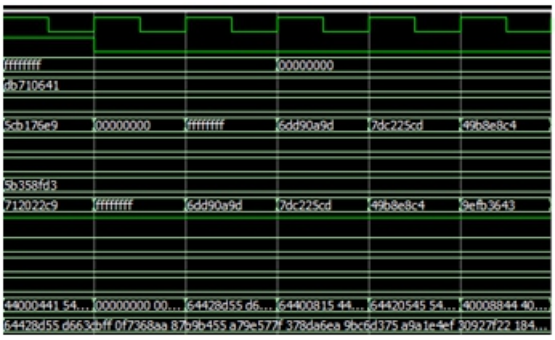


Figure.8: Simulation result of 64 bits processing

Input applied at first clock cycle is all zeros and the after making the rst low the input applied as the FFFFFFFF for the two clock cycles. After two clock cycles the input makes all zeros for the polynomial neutralization then the output occurred after two clock cycle.

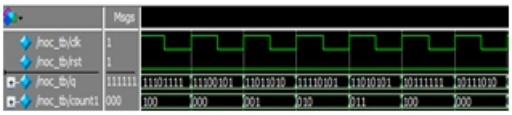


Figure9.simulation result of novel test pattern

In test mode the inputs are applied from the LFSR and the flop is connected in test mode the outputs are given to the response analyzer for the validation. The same output is connected form the pattern generation to response analyzer for testing.In test mode the inputs are applied from the LFSR and the flop is connected in test mode the outputs are given to the response analyzer for the validation. The same output is connected form the pattern generation to response analyzer for testing.

V.CONCLUSION:

Parallel CRC calculation circuit for the cryptographic system is designed based on the Novel test mechanism which gives the better performance with reference with the traditional test mechanisms. The test patterns can be generated with the LFSR automatic test pattern generator and verification can be done at the response analyzer with same LFSR outputs with the flop outputs. The proposed circuit runs well for the normal mode as well as the test mode efficiently. Our design testing can be done only for the flops.

VI REFERENCES:

[1].Elena Dubrova , Mats N¨aslund and G¨oran Selander "Secure and Efficient LBIST for Feedback Shift Register-Based Cryptographic Systems" 2014 19th IEEE European Test Symposium (ETS)
[2].T. Good and M. Benaissa, "ASIC hardware performance," New Stream Cipher Designs: The eSTREAM Finalists, LNCS 4986, pp. 267–293, 2008.
[3].G. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopantlevel hardware Trojans," Proceedings of Cryptographic Hardware and Embedded Systems (CHES'2013), LNCS 8086, pp. 197–214, 2013.
[4].T. W. Cusick and P. St˘anic˘a, Cryptographic Boolean functions and applications. San Diego, CA, USA: Academic Press, 2009.
[5].S. Reddy, "Easily testable realizations for logic functions," IEEE Transactions on Computers, vol. 21, no. 11, pp. 1183–1188, 1972.
[6].R. K. Brayton, C. McMullen, G. Hatchel, and A. Sangiovanni- Vincentelli, Logic Minimization Algorithms For VLSI Synthesis. Kluwer Academic Publishers, 1984.
[7].M. Abramovici, M. A. Breuer, and A. D. Friedman, Digital Systems Testing and Testable Design. Jon Willey and Sons, New Jersey, 1994.
[8].D. H. Green, "Families of Reed-Muller canonical forms," International Journal of Electronics, vol. 70, pp. 259–280, 1991.
[9].C. Canni`ere and B. Preneel, "Trivium," New Stream Cipher Designs: The eSTREAM Finalists, LNCS 4986, pp. 244–266, 2008.
[10].Giuseppe Campobello, Giuseppe Patane` , and Marco Russo "Parallel CRC Realization" IEEE Transactions On Computers, Vol. 52, No. 10, October 2003
[11].W.W. Peterson and D.T. Brown, "Cyclic Codes for Error Detection," Proc. IRE, Jan. 1961.
[12].A.S. Tanenbaum, Computer Networks. Prentice Hall, 1981.
[13].W.Stallings, Data and Computer Communications. Prentice Hall, 2000.
[14].T.V. Ramabadran and S.S. Gaitonde, "A Tutorial on CRC Computations," IEEE Micro, Aug. 1988.