Recent Developments in Electronics and Communication Systems
KVS Ramachandra Murthy et al. (Eds.)

doi:10.3233/ATDE221311

BIST Application of DCM Based True Random Number Generator

Muthyala Sowmika[1,a)],Manchalla.O.V.P.Kumar [2,b)] , Kiran Mannem [3,c)], K. Jamal[4,d)]
[1]*M.Tech Scholar, 1Department of ECE, GRIET, Hyderabad, India.*
[234]*Department of ECE, GRIET, Hyderabad, India.*
[a)]*msowmika@gmail.com*

Abstract. A hardware random number generator is designed with the help of digital clock manager. The number is evenly distributed in a random manner. Each number in the series is individualistic. The generated random number is unpredictable. Therefore they are used in key generation. Such keys are used to secure the transferred information. Built - in self test is an application of TRNG. Built - in self testing enables the circuit to test for any faults. BIST is a procedure where a circuit is designed so that it tests itself and describes whether it is faulty or fault free. A true random number which is generated using DCM is put in the circuit which is under testing. The corresponding circuit is vedic multiplier. The faults in the circuit under test are detected using built-in self test process. The software tool used for programming part is Xilinx suite 14.3.

1. Introduction.

A digital system must be tested for any failures in various occasions. Testing must be as fast as possible and to achieve that, the testing is made as a function of system. Thus called as self - test. Built - in self testing is a process of designing a circuit so that it examines itself. The name BIST originates from the plan of including Pseudo Random number generator with cyclic redundancy check in the integrated circuits. Various cryptographic protocol flaws exists [5].

Built - in self test mechanism can be used for testing communication systems. A hardware random number generator is designed using DCM.The analysis of such DCM based true random number generator has been proposed [1].The random number is used to generate keys to secure the transferred information. Thus through these secret keys the system is made robust against various attacks[3].In general, crypto chips need to be tested for faults. To test them, built in self test architecture is proposed[2].Built-in self test mechanism is applied to the hardware random number generated.The generated true random number is applied to the circuit under test. The circuit under test which is a vedic multiplier is tested for faults. Built - in self testing block diagram consists of three main blocks. Those are the test pattern generator(TPG), circuit under test (CUT) and the output response analyzer (ORA). Each of the block has its own significance and plays a crucial role in the testing process.

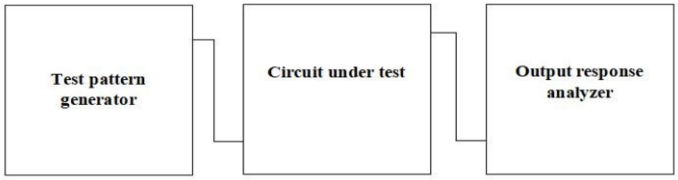

Figure 1. Block diagram of BIST

1.1 Vedic Multiplier.

Vedic multiplier which is designed in order to perform digital multiplication. Such method is different from multiplication that involves add and shift.

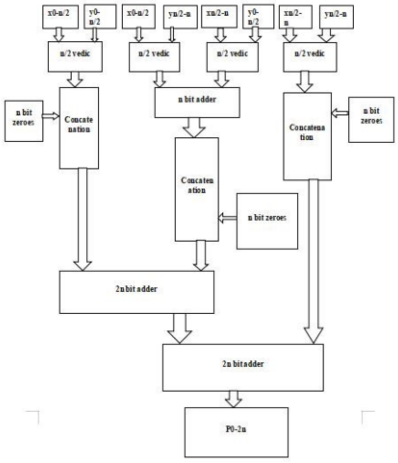

Figure 2. N bit Vedic multiplier

Here vedic multiplier with 'n' number of bits. It contains four n/2 multipliers which are used for calculating the partial products. In order to obtain all the partial products of equal length the results from these n/2 multipliers are modified. The partial product from the rightmost multiplier and the partial product from the leftmost multiplier are concatenated with each other. Similarly the partial products from the middle multipliers are concatenated. All the numbers obtained from concatenation are added together using a 2n bit adder. And finally the result obtained from 2n bit adder is concatenated with the least significant bit of the rightmost multiplier and added using 2n bit adder to obtain the final product.

2. Literature review.

E. Bohl and **M.Ihle.**"A Fault Attack robust TRNG".2012, IEEE. In this paper a Fault attack robust TRNG is proposed. True Random number generators are used in cryptographic systems. They generate secret keys and these secret keys make the design

robust against the attacks. To understand father attacks easily, some bias is introduced in the uniform distribution of TRNG output. Fault attacks can be detected and an error signal indicates fault which is a permanent frequency correlation of an oscillator.

Marion Doulcier and **Bruno Rouzeyre**. "Self-Test Techniques for Crypto-Devices"."IEEE Transactions on very large scale integration systems, vol.18,no.2 february 2010"In this paper, built - in self test process for devices with symmetric to cryptographic core has been proposed. The self test process involves, applying the core with it's own output and letting the device to run for a number of encryptions and comparing the final output with reference signature. It gives the advantage of 100% fault coverage on the crypto- cores and with no overhead.

Berk Sunar and **William J. Martin .**"A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks"."IEEE transactions on Computers, vol. 56, no. 1, january 2007."In this paper, fault tolerance of random bit generator against attack has been presented. The basic idea is to improve the fill rate. For this purpose, more number of oscillators are required. Random bits with notably some tolerance to attacks are generated. The analysis based on methods to improve the performance of design has been proposed here.

Jamal. K, Srihari. P, and **Kanakasri. G.** "Test Vector generation using Genetic Algorithm for Fault Tolerant systems. 2016".In this paper, a genetic algorithm is proposed in order to produce patterns automatically. This is done to detect faults in memory. It is efficient algorithm in detecting perfect number of test patterns. However the test sets generated by such algorithm are tightly packed.

3. Methodology.

A DCM based hardware random number generator is designed. The basic principle is beat frequency detection. A digital clock manager is used to provide clock signals. It is also used to manage those clock signals. It avoids clock skew, where the clock signals reach the components at different times. Therefore it facilitates for improved performance.

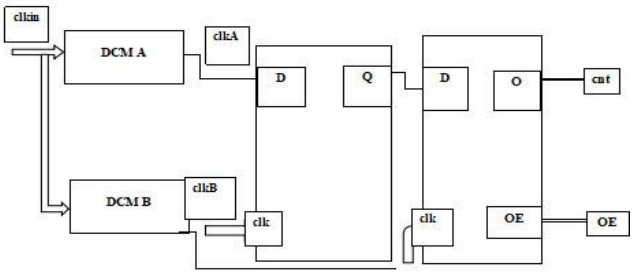

Figure 3. DCM Block diagram

Here two DCM signals are used. They are connected to the delay flip flop. One signal being connected as input to the flip flop and the other is connected as clock signal to the flip flop. According to the functionality of DCM, two signals are generated with different clock frequencies. The difference between these clock frequencies is detected by the principle of beat frequency detection. Based on the working principle of the delay flip flop, the output of the delay flip-flop becomes the repetition of zeroes and ones. The necessity of the counter here is that, it counts the number of successive logic ones and displays it at the output. The output is then sampled by using a sampling clock. The true random number is generated from the sampling response.

The hardware random number which is generated using DCM is applied to BIST mechanism. Built in self testing is a process where the circuit is tested to determine whether it is faulty or fault free. A true random number generator is the circuitry which provides the test patterns for the circuit which is to be examined. It also involves providing a procedure which determines the output response is faulty or fault free with respect to the generated test patterns. BIST architecture basically consists of two essential functional blocks namely test pattern generator(TPA) and output response analyser (ORA).

The test pattern generator generates the sequence of patterns in order to test the circuit. The analysis of test pattern generator is proposed [4].The true random number generator based on DCM is used as the test pattern generator And it is used to provide input test vectors to the circuit under test. The circuit under test which is used for the testing process is Vedic multiplier. The 8bit random number which are generated by TRNG are given as input to the Vedic multiplier which is the circuit under test. Vedic multiplication is performed the 8 bit random number by using a 4×4 vedic bit vedic multiplier.

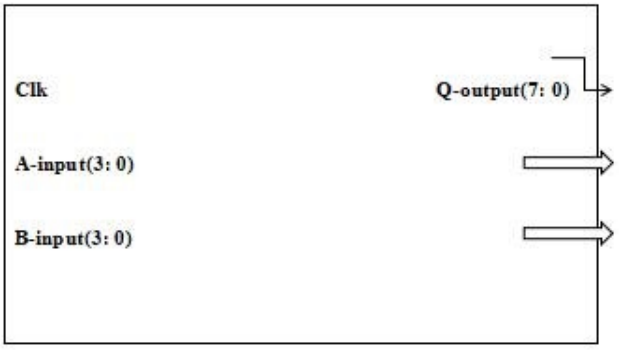

Figure 4. A 4×4 vedic multiplier

The corresponding output is stored in output response analyser. The output response analyzer compresses the output of the circuit under test into a signature. It compares it with the golden signature to determine the circuit behaviour. Hence it is also called as signature analyzer. From the comparison the circuit under test is determined to be faulty or fault free.

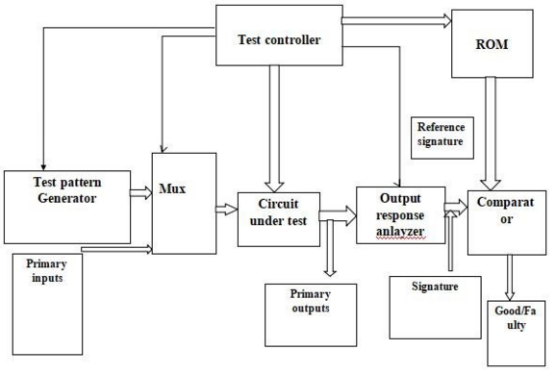

Figure 5. BIST Architecture

From the architecture of BIST, functional blocks like multiplexer, test controller, response compactor are observed. Each block has its own significance in BIST implementation. The test controller is used to control the test pattern and generation of test during BIST mode. Primary inputs in the architecture are the inputs for the circuit under test in non-BIST mode. During the BIST mode, an isolation circuitry is used in order to select the input signals for the circuit and test. Therefore in BIST mode, the multiplexer selects inputs from the test pattern generator and in non-BIST mode, it selects primary inputs. Several pattern generation techniques like TPC are proposed [6].

The response compactor is a compactor which reduces the circuit response into manageable size. It is necessary to compact the response because the comparison is a tedious and time consuming process. Hence the response is compacted and used as a signature and compared with the reference signature from multiplier. If both the results are matched then the circuit is said to be free from fault. If mismatched then the circuit is said to be having fault. The presence of fault in the circuit is detected and indicated as fail, whereas the absence of fault in the output is indicated as pass. Thus the fault is detected through BIST mechanism.

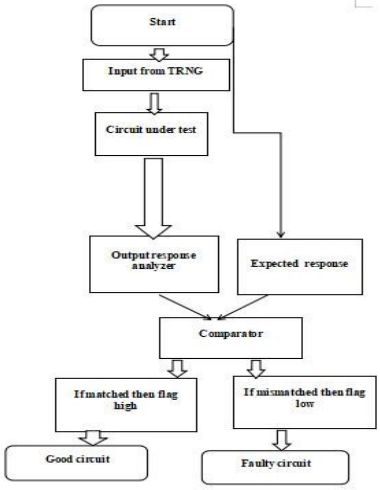

Figure 6. Implementation flow of BIST

At the start of the implementation test vectors are applied to the true random number generator and the true random number is given as input to the circuit which is Vedic multiplier. Vedic multiplication is performed on the corresponding random number and output is stored in the output response analyser. The corresponding output response is compared with the expected response of the reference circuit multiplier using comparator and if there is a match flag remains high and the circuit is said to be fault free circuit. If in case the mismatch occurs then the circuit is said to be faulty and the flag remains low. The faulty positions in the output response are indicated as fail.

4. Results and Discussion.

The simulation process of this project has been carried out in XILINX ISE DESIGN SUITE14.7 version software tool. The corresponding steps required for implementing the design is shown.

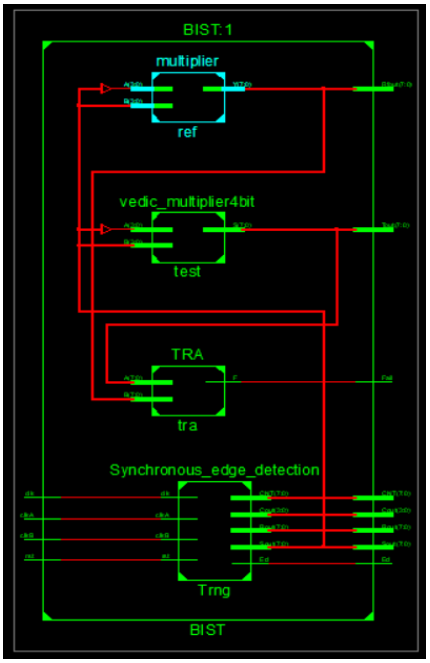

Figure 7. RTL Schematic

After completion of implementing the code, check syntax in order to check the syntactical errors and flaws that are present in the program. The third step is to click on the view RTL schematic to verify the RTL of the implemented code. The fig. above shows the RTL schematic of the BIST mechanism for DCM based true random number generator.

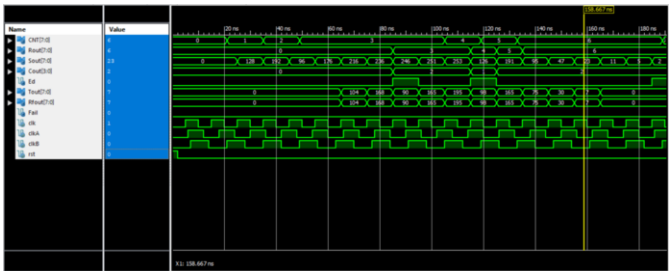

Figure 8. Simulation Results

The simulation results of the corresponding BIST mechanism for DCM based true random number generator. This work discusses the number of test vectors needed to find the faults present in the multiplier. These are the final results which represent the presence of fault as fail indication and absence of fault as pass indication.

5. Conclusion

A true random number has been generated using a digital clock manager. An 8 bit random number is generated. The generated random number is applied to the built-in self test mechanism. BIST is an application of true random numbers generator. The test pattern generator is used to generate the input stimulus to the circuit under test. The circuit under test used here is a vedic multiplier. Multiplication is performed by using one of the sutras of vedic mathematics. The output response analyzer is used to produce the output of the circuit. The output response is then compared with the expected response using comparator. The reference circuit through which the expected response is generated is a multiplier. As the circuit under test used is the vedic multiplier, the corresponding output response of Vedic multiplier is compared with the expected response of multiplier. If the presence of fault is detected then the circuit under test is said to be faulty. In this manner a fault has been detected in the circuit under test and the changes in the output response are observed as pass and fail indications.

References

[1] A.P. Johnson, R. S. Chakraborty, and D. Mukhopadyay, “An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA,”IEEE Transaction on Circuits and Systems II: Express Briefs, vol. 64,no. 4, pp. 452–456, 2017.

[2] B.Yang and R. Karri, “Crypto BIST: A built-in self test Architecture for crypto chips,” in Proc. 2Nd Workshop on Fault Diagnosis Tolerance Cryptography (FDTC), 2005, pp. 95–108.

[3] E. Boehl and M. Ihle. A Fault attack robust TRNG. In On- LineTesting Symposium, 18th IEEE International, 2012.

[4] Jamal, K., & Srihari, P. (2015, January). Analysis of test sequence generators for built-in self-test implementation. In2015 International Conference on Advanced Computing and Communication Systems (pp. 1-4). IEEE.

[5] U. Carlsen, “Cryptographic protocol flaws,” in IEEE Compute Security Foundations Workshop, Franconia, New Hampshire, 1994.

[6] Jamal, K., Chari, K. M., & Srihari, P. (2019). Test pattern Generation using thermometer code counter in TPC technique for BIST implementation. Microprocessors and Microsystems, 71, 102890.