International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 5, Sept-Oct 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

DESIGN OF TRUE RANDOM NUMBER GENERATOR BASED ON MULTI-STAGE FEEDBACK RING OSCILLATOR

Viveka.S*, Dr. V.Kalaipoonguzhali,**

*(PG Scholar VLSI/Sembodai Rukmani Varatharajan Engineering College, and Sembodai, Email:vivekala1313@gmail.com)

**(Professor and HOD of ECE, /Sembodai Rukmani Varatharajan Engineering College, and Sembodai, Email: hodeeesrvec@gmail.com)

----------**********----------

Abstract:

True random number generators (TRNGs) play an important role in VLSI Testing. In a innovative method of generating true random numbers on a field programmable gate array (FPGA) is planned based on the random jitter of a multi-stage feedback ring oscillator (MSFRO) as the entropy source. Created on the old-style ring oscillator a multi-stage feedback assembly is added to increase the range of clock jitter, and improve the frequency of clock sampling and the randomness of the information source. Changed from the traditional clock sampling structure, we use the clock jitter signal produced by the MSFRO to sample the clock signal generated by the phase-locked loop (PLL) of the FPGA. The found output value is operated by XOR to reduce the deviation of the output value and progress its randomness. MSFRO are presented to demonstrate the performance of the proposed LP BIST approach. This Proposed design will be implemented by Verilog HDL and simulated by Modelsim Tool. The Proposed MSFRO is Synthesis by Xilinx and FPGA Spartan 3 XC 3S 200 TQ 144.

Keywords —Encryption,Decryption,FPGA,HDL, PLL,TRNGs,MSFRO, LP BIST.

----------**********----------

I. INTRODUCTION

The gap between functional and test power consumption is growing bigger and bigger, with the latter reaching 2X to 5X of the former due to the ever-shrinking functional power and ever-increasing test power . Problems, such as excessive heat that may reduce circuit reliability, formation of hot spots, difficulty in performance verification, reduction of the product yield and lifetime, and so on, have become severe .. A fast simulation approach was proposed for low-power (LP) off-chip interconnect design. An important through silicon via (TSV) modeling/simulation technique for LP 3- D stacked IC design .Furthermore, the power dissipation of scan-based built-in self-test (BIST) is much higher than power degeneracy in deterministic scan testing due to excessive switching actions caused by random designs. it is essential to propose an active LP BIST approach. Though, many of the earlier LP BIST approaches cause fault attention loss to some extent. Therefore, achieving high fault coverage in an LP BIST scheme is also very important. Weighted pseudorandom testing schemes and methods can effectively improve fault coverage. However, these approaches usually result in much more power consumption due to more frequent transitions at the scan flip flops in many cases. Therefore, we intend to propose an LP scan-based pseudorandom pattern generator (PRPG).

II. LITERATURE SURVEY-1:

TITLE : Bit-Swapping LFSR and Scan-Chain Ordering: A Novel Technique for Peak- and Average-Power Reduction in Scan-Based BIST

AUTHOR : Abdallatif S. Abu-Issa and Steven F. Quigley

YEAR : May 2009

DESCRIPTION: This article presents a novel low-transition linear feedback shift register (LFSR) it is based on some new explanations about the output sequence of a conventional LFSR. The proposed design, called bit-swapping LFSR (BS-LFSR), is composed of an LFSR and a 2 × 1 multiplexer. When used to generate test patterns for scan-based built-in self-tests, it reduces the number of transitions that occur at the scan-chain input during scan shift operation by 50% when likened to those patterns produced by a conventional LFSR. Hence, it decreases the overall switching activity in the circuit under test during test applications. The BS & LFSR united with a scan-chain-ordering algorithm that orders the cells in a way that reduces the average and peak power in the test cycle or while scanning out a response to a signature analyzer. These methods have a substantial effect on average and peak power reductions with negligible effect on fault coverage or test application time. Experimental results on ISCAS'89 benchmark circuits show up to 65% and 55% reductions in average and peak power, respectively..

III. LITERATURE SURVEY-2:

TITLE : Adaptive Low Shift Power Test Pattern Generator for Logic BIST

AUTHOR : Xijiang Lin Janusz Rajski

DESCRIPTION:Increasing the connection amongst adjacent test stimulus bits can significantly decrease shift power consumption. it often causes test attention loss when applying it to reduce the shift power feeding in logic BIST. In this paper, a new adaptive low shift power random test pattern generator (ALP RTPG) is presented to progress the tradeoff between test coverage loss and shift power decrease in logic BIST. This is achieved by applying the information derived from test responses to dynamically adjust the correlation among adjacent test stimulus bits. When comparation an existing method, called LT RTPG, investigational results for industrial designs show that the planned method can significantly reduce the test exposure loss while still achieving dramatic shift power reduction..

IV. EXISTING SYSTEM:

- A weighted test enables signal based pseudorandom test pattern generation scheme.

practice.

V. EXISTING SYSTEM DRABACKS:

- False test fail may be generated, with consequential increase in produce loss
- it requires a momentous increase in number of test vectors
- consequently, test time, to achieve the same Fault Coverage (FC)as with conventional scan based LBIST

VI. PROPOSED SYSTEM:

TRNG structure uses two MSFROs as the jitter signal source. The PLL generates two normal clocks. The output of PLL is used as the data input of flip-flop, and the output of MSFRO is used as the clock signal input of flip-flop. Each time the rising edge of the MSFRO output signal comes, the D flip-flop will sample the PLL output signal to generate one random bit. The phase jitter range caused by noise is very small, and many definite values will be sampled when using the trigger to sample, which will reduce the randomness of random numbers. Therefore, the proposed TRNG uses two MSFRO as the entropy source, and directly obtains random numbers by XOR output after extracting their randomness. New LP deterministic BIST structure is planned to encode the deterministic test designs for random pattern and resistant faults. Only a part of flip flops are activated in each cycle of the whole process of deterministic BIST.

A new LP weighted pseudorandom test pattern originator using weighted test enable signals is planned using a new clock inactivating scheme. The design for testability (DFT) architecture to implement the LP BIST scheme is presented. Our method produces a series of dishonored sub circuits. The new LP BIST scheme selects weights for the test-enable signals of all scan chains in each of the degraded sub circuits, which are activated to maximize the testability.

New LP deterministic BIST scheme is proposed to encrypt the deterministic test patterns for random pattern and resistant faults. Only a part of flip flops are activated in each cycle of the whole process of deterministic BIST. A new procedure is proposed to select a primitive polynomial and the number of extra variables injected into the linear-feedback shift register (LFSR) that encode all deterministic patterns. The new LP reseeding scheme can cover a number of vectors with fewer care bits, which allows a small part of flip flops to be activated in any clock cycle.

VII. PROPOSED SYSTEM ADVANTAGES:

- Lower test time area overhead while running.
- While requiring a meaningfully lower test time and comparable area overhead
- It does not rise the number of test vectors
- It requires a small cost in relations of area overhead

VIII. SYSTEM ARCHITECTURE:

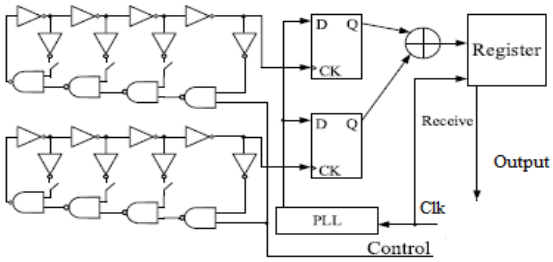

Fig. 1System Architecture

IX. CONCLUSIONS

A latest LP BIST method has been proposed using weighted test enable signal-based pseudorandom test pattern peers and LP deterministic BIST and reseeding. The new method consists of two separate stages. One is LP weighted pseudorandom pattern generation and the second one is LP deterministic BIST with reseeding. The first phase chooses weights for test enable signals of the scan cuffs in the triggered sub circuits. A new procedure has been proposed to select the primitive polynomial and the number of extra inputs injected at the LFSR. A new LP reseeding scheme, which guarantees LP operations for all clock cycles, has been proposed to further reduce test data kept on-chip. Experimental results have demonstrated the performance of the proposed method by comparison with a recent LP BIST method. The LP reseeding technique is a little more complicated. This work can be extended to latch-on-capture transition fault testing and small delay defect testing.

REFERENCES

[1] [1] A. S. Abu-Issa and S. F. Quigley, "Bit-swapping LFSR and scan-chain ordering: A novel technique for peak- and average-power reduction in scan-based BIST," IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol. 28, no. 5, pp. 755–759, May 2009.

[2] [2] V. D. Agrawal, C. R. Kime, and K. K. Saluja, "A tutorial on built-in selftest. I. Principles," IEEE Des. Test Comput., vol. 10, no. 1, pp. 73–82, Mar. 1993.

[3] [3] A. Al-Yamani, N. Devta-Prasanna, E. Chmelar, M. Grinchuk, and A. Gunda, "Scan test cost and power reduction through systematic scan reconfiguration," IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol. 26, no. 5, pp. 907–918, May 2007.

[4] [4] Synopsys, ASTRO: Advanced Place-and-Route Solution for SoC Design, accessed on Mar. 1, 2015. [Online]. Available: http://www.synopsys.com/products/astro/astro.html

[5] [5] S. Banerjee, D. R. Chowdhury, and B. B. Bhattacharya, "An efficient scan tree design for compact test pattern set," IEEE Trans. Comput.- Aided Des. Integr. Circuits Syst., vol. 26, no. 7, pp. 1331–1339, Jul. 2007.

[6] [6] P. H. Bardell, W. H. McAnney, and J. Savir, Built in Test for VLSI: Pseudorandom Techniques. New York, NY, USA: Wiley, 1987.

[7] [7] N. Z. Basturkmen, S. M. Reddy, and I. Pomeranz, "A low power pseudorandom BIST technique," J. Electron. Test., Theory Appl., vol. 19, no. 6, pp. 637–644, Dec. 2003.

[8] [8] M. L. Bushnell and V. D. Agrawal, Essentials of Electronic Testing.Norwell, MA, USA: Kluwer, 2000.

[9] [9] M. Chatterjee and D. K. Pradhan, "A BIST pattern generator design for near-perfect fault coverage," IEEE Trans. Comput., vol. 52, no. 12, pp. 1543–1558, Dec. 2003.

[10] M. Filipek et al., "Low-power programmable PRPG with test compression capabilities," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 6, pp. 1063–1076, Jun. 2015.

