International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Secure Fault Diagnosis for Framework on Chip Design and Testing

B. Swapna, M. Kamalahasan, Rishi Mishra, Dipankar Singh, Adnan umar mallick

Abstract - Because of the extensive expense of semiconductor fabricating, most framework on-chip structure organizations redistribute their generation to seaward foundries. As a large portion of these gadgets are fabricated in situations of constrained trust that regularly need suitable oversight, various diverse dangers have risen. These incorporate unapproved overabundance of the ICs, offer of out-of-determination/rejected ICs disposed of by assembling tests, robbery of scholarly property, and figuring out of the structures. The Boolean calculations are effectively break key-based confusion techniques and therefore go around the essential destinations of metering and confusion. In this research paper, we present an innovation secure cell plan for executing the structure for-security foundation to avoid releasing the way to a foe under any conditions and produce fault free integrated circuit design. Our proposed structure is impervious to different known assaults at the expense of a next to no region overhead. This Proposed Framework Actualized utilizing Verilog HDL also recreated by Modelsim 6.4 c and Integrated by Xilinx device.

Keyword - Fault analysis, Integrated circuits, secure cell, security key and Arithmetic and logic units (ALU).

I. INTRODUCTION

An epic secure cell plan for executing the structure for-safety framework to anticipate releasing the way to a foe under any conditions are assigned. Significantly, our plan cannot confine the testability of the chip amid the ordinary assembling stream in any capacity, including post silicon approval and investigate. Design and Test the combinational and sequential circuit with fault and without fault in the proposed work.

II. LITERATRE SURVEY

Low-progress linear feedback shifts register (LFSR) depends on some new perceptions regarding yield grouping of a traditional LFSR. The given structure, called bit-swapping LFSR (BS-LFSR), is made out of a LFSR and a 2*1 multiplexer.

Revised Manuscript Received on March 30, 2020.
***** Correspondence Author
B. Swapna*, Assistant Professor, Electronics and Communication Engineering, Dr MGR Educational and Research Institute, Chennai, India. Email: swapna.eee@drmgrdu.ac.in
M. Kamalahasan, Research Engineer, Advanced Research Institute, Dr MGR Educational and Research Institute, Chennai, India. Email: kamal.ari@drmgrdu.ac.in
Rishi Mishra, UG Scholar, Dr MGR Educational and Research Institute, Chennai, India
Dipankar singh, UG Scholar, Dr. MGR Educational and Research Institute, Chennai, India
Adnan umar mallick, UG Scholar, Dr MGR Educational and Research Institute, Chennai, India

At the point when used to create test designs for sweep based implicit individual tests, it lessens the quantity of changes that happen at the output chain contribution amid sweep move activity by half when contrasted with those examples delivered by a customary LFSR [2]. Segmented addressable scan (SAS), a test design that tends to test information volume, test application time, test control utilization, and analyzer channel prerequisites utilizing an equipment aerial of a couple of gates per examine chain. Utilizing SAS, it additionally shows orderly sweep reconfiguration, a test information pressure calculation that is connected to accomplish 10× to 40× pressure proportions without requiring any data from the programmed investigate-design age instrument about the undefined bits. The engineering and the calculation were connected to both single stuck and also progress fault test set [3].

Tree-based output way designs have as of late been proposed for lessening test application time or test information volume in the present high-thickness extensive scale coordinated circuits. Nonetheless, these methods firmly depend on the presence of a substantial number of perfect arrangements of flip-tumbles under the given test set and hence may not be appropriate for an exceptionally reduced test set created by an effective programmed test design generator apparatus. Tree-based structures additionally experience the ill effects of loss of fault coverage while accomplishing a huge decrease proportion for test time or information. In this paper, to evade this issue, another two-pass crossover strategy is proposed to structure a proficient sweep tree engineering dependent on inexact similarity. The strategy is especially appropriate for a much minimized test set having less don't considerations and low similarity. At long last, to lessen the volume of sweep out information, test reactions moved out from the leaf hubs of the output tree are compacted by a space compactor, which is structured extraordinarily for the proposed sweep tree design. The compactor utilizes a XOR tree, and its overhead is low. The structure along these lines offers an answer for both test information and reaction compaction and application time altogether without corrupting faults coverage [4].

Another structure system for an example generator is proposed, detailed with regards to on-chip BIST [5]. The plan system is circuit-particular and utilizations blend methods to structure built in Self-Test generators. The example generator comprises of two parts: a pseudorandom design generator (like a LFSR or, ideally, a GLFSR) and a combinational logic to outline yields of the pseudorandom design generator. This combinational logic is integrated to create a given arrangement of target designs by mapping the yields of the pseudorandom design generator.

It is demonstrated that, for a specific CUT, n area-efficient combinational logic square can be planned/integrated to accomplish 100 (or right around 100) percent single stuck to fault coverage utilizing few test designs.

This strategy is fundamentally not quite the same as weighted example age and it ensure testing of all. It is difficult to-distinguish deficiencies without costly investigate point inclusion. Test results on regular benchmark net lists show that the fault coverage of the proposed example generator is fundamentally higher contrasted with ordinary example age procedures. The plan system for the rationale mapper is one of a kind and it is utilized to enhance existing example alternators for combinational logic and output based BIST structures [5].

It is involved a straight limited state machine (a direct input move enlist or a ring generator) driving a suitable stage shifter, and it accompanies various highlights enabling this gadget to create twofold groupings with preselected flipping (PRESTO) action. We acquaint a technique with consequently select a few controls of the generator offering simple and exact tuning. A similar system is hence utilized to deterministically control the generator toward test arrangements with enhanced fault coverage to design check proportions. Besides, this paper proposes a LP test pressure technique that permits molding the test control envelope in a completely unsurprising, precise, and adaptable form by adjusting the PRESTO-based rationale BIST (LBIST) foundation.[17][6] The proposed mixture conspire effectively consolidates test pressure with LBIST, where the two methods can work synergistically to convey great tests [6].

The increasing power utilization amid the chip testing method has become the bottleneck of chip creation and testing for miniaturized scale nano VLSI circuits. Varied low power style for-testability (DFT) systems are projected to manage the check management issue, and fragmented output strategy was looked as if it would be a productive arrangement. We have a tendency to propose another power output section style, which may exactly management the intensity of move and catch cycles within the in the meantime. Since empowering simply a set of sweep flip-lemon to catch check reactions during a single cycle bargains the fault coverage, we have a tendency to propose another strategy to reduce the fault coverage misfortune. to start with, we have a tendency to utilize an additional precise thought, ruined hubs, instead of infringement edges used in past tries to interrupt down the reliance of flip-flops, at that time we have a tendency to utilize simulated tempering (SA) part to find the most {effective} mix of those flip-flops whereas considering the clock trees' effect. To the simplest of our insight, this can be the first work to form move and catch management controllably with least fault coverage misfortune, very little check-information volume and no extra instrumentation overhead for at-speed progress fault test. Broad analyses are performed on reference circuit ISCAS89 and IWLS2005 to verify the viability of the projected strategy [7].

III. PROPOSED WORK

Design and test (fault analysis) the combinational logic circuits ICs with the help of secure cell and DFS technique.

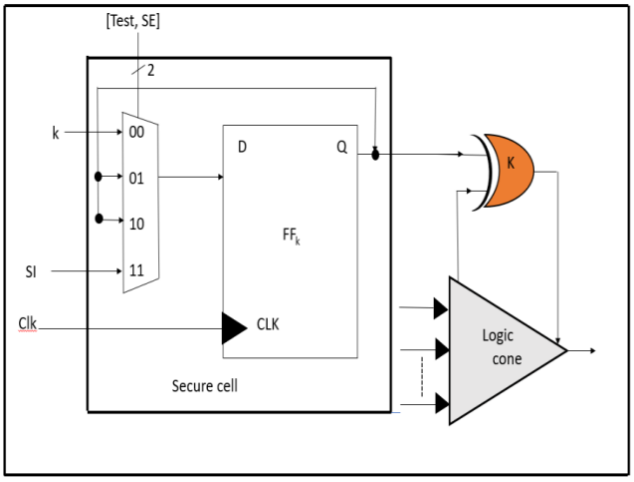

Fig.1. Proposed Secure cell Block Diagram for testing [1]

A. Multiplexers

A multiplexer (or mux) is a gadget that chooses one of a few simple or advanced information flags and advances the chosen contribution to a solitary line. A multiplexer of 2n inputs has ⌈n⌉ select lines, which are utilized to choose which input line to send to the yield.

B. Register

Registers can be organized utilizing unmistakable Flip-Flops (S-R or J-K as D-type) and are in like way accessible as MSI contraptions. Registers in which information are taken out in progressive edge are proposed as move library, since bits are moved in the Flip-Flops with the event of check beats either the correct way or in the left heading or in both the course.

C. Combinational Circuit Testing

In Enhancement we will execute an Arithmetic Logical Unit (ALU) with BIST capacity; ALU involving distinctive math activities and coherent tasks is actualized. ALU is utilized in many handling and processing gadgets, because of quick advancement of innovation the quicker number juggling unit is required as well as less territory and low power number-crunching units are required and because of the expanding combination complexities of IC's the Optimized ALU actualized some of the time may mal-work, so testing capacity must be given and this is expert by Built In Self-Test (BIST) for Optimized ALU. Area develops an ALU from four equipment building squares (AND as well as gates, inverters, and multiplexors) and outlines how combinational rationale works [20].

D. Xor Logic

The XOR gate (at times EOR gate, or EXOR gate and articulated as Exclusive OR gate) is a computerized rationale gate that executes a selective or; that is, a genuine yield (1/HIGH) results in the event that one, and just a single, of the contributions to the gate is valid. In the event that the two data sources are false (0/LOW) and both are valid,

a false yield results. XOR speaks to the disparity work, i.e., the yield is valid if the sources of info are not alike generally the yield is false. An approach to recollect XOR is "either however not both".

XOR can likewise be seen as expansion modulo 2. Subsequently, XOR gates are utilized to execute paired expansion in PCs. A half adder comprises of a XOR gate and an AND gate. Different utilizations incorporate subtractors, comparators, and controlled inverters.

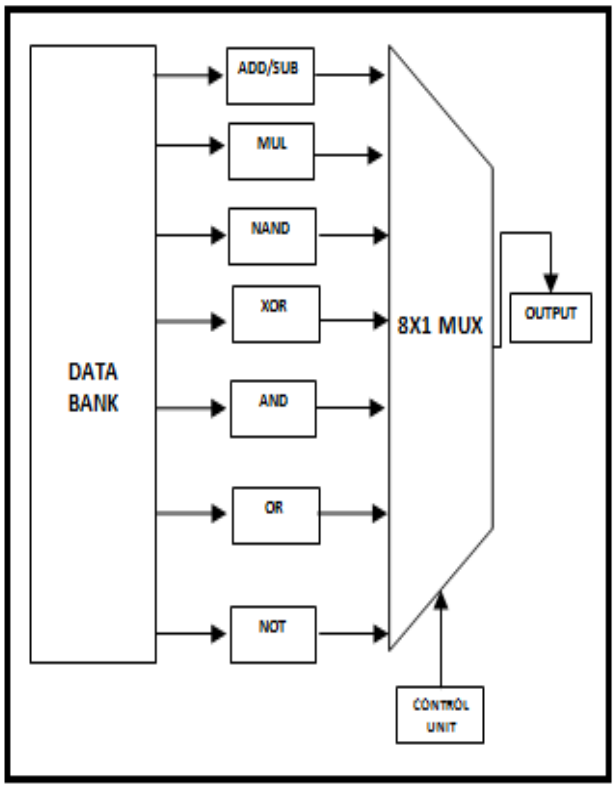

Fig.2. Combinational Circuits – Accumulator Testing

E. Modules

- AND Logic
- OR Logic
- Adder
- Multiplier
- ALU

1. And Rationale

The AND fence is a fundamental computerized rationale gate that executes consistent combination - it carries on as per reality table to one side. A HIGH yield (1) results just if both the contributions to the AND gate are HIGH (1). On the off chance that neither or just a single contribution to the AND gate is HIGH, a LOW yield results. In another sense, the capacity of AND adequately finds the base between two double digits, similarly as the OR work finds the most extreme. Thusly, the yield is dependably 0 with the exception of when every one of the data sources is 1.

2. Or Logic

The OR gate is an advanced rationale gate that actualizes coherent disjunction - it acts as per reality table to one side. A HIGH yield (1) results in the event that one or both the contributions to the gate are HIGH (1). In the event that neither one of the inputs is high, a LOW yield (0) results. In another sense, the capacity of OR viably finds the most extreme between two parallel digits, similarly as the reciprocal AND capacity finds the base.

3. Surge Carry Adder

Various full adder circuits can be fell in parallel to incorporate a N-bit number. For a N-bit parallel snake, there must be N number of full adder circuits. A swell pass on adder is a justification circuit in which the total of each full snake is the pass on in of the predominant next most vital full adder. It is known as a swell pass on adder in light of the way that each pass on information gets undulated into the accompanying stage. In a swell pass on snake the aggregate and do bits of any half adder mastermind isn't real until the passes on in of that arrange occurs.

Spread deferments inside the method of reasoning equipment are the clarification for this. Proliferation delay is time snuck past between the use of a data and occasion of the relating yield. Consider a NOT entryway, When the data is "0" the yield will be "1" and the different way. The time taken for the NOT entryway's respect twist up "0" after the use of method of reasoning "1" to the NOT door's data is the proliferation delay here. Correspondingly the pass on spread postponement is the time snuck past between the use of the pass on in banner and the occasion of the do (Cout) hail. Circuit diagram of a 4-bit swell pass on snake is exhibited as pursues.

4. Multiplier

Multiplier unit is upgraded utilizing Vedic Multiplier strategy this builds speed and declines control.

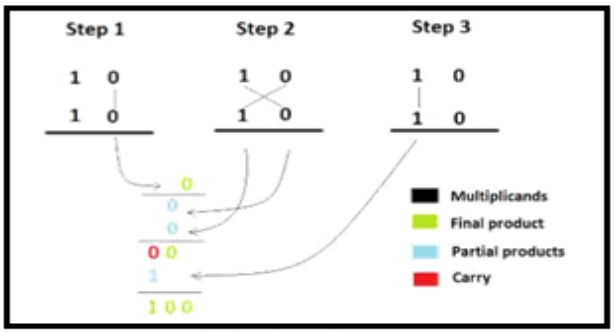

Fig.3. Multiplier Representation

5. Alu

This region presents the refined structure of a reversible n-bit ALU reliant on a controlled quantum full adder proposed by Kai-Wen Cheng et al. with a progressive strategy of tasks[16]. The proposed reversible ALU hopes complete the accompanying fundamental game plan of assignments,

- ADD activity: | A + B
- SUB activity: | A - B;
- Negative SUB activity: | B − > A;
- Bitwise elite or operation:| A ⊕ B
- OR activity: | A or B
- AND activity: | A and B [16]

IV. IMPLEMENTATION AND RESULTS

A. Combinational Circuit testing

In Enhancement we are going to implement a Arithmetic Logical Unit (ALU) with BIST capability, ALU comprising of different arithmetic operations and logical operations is implemented. ALU is employed in several processes and computing devices, because of speedy development of technology not solely the quicker arithmetic unit is needed however additionally less space and low power arithmetic units area unit required and because of the increasing integration complexities of IC's the Optimized ALU enforced generally might mal-function, so testing capability must be provided and this is accomplished by in-built Self check (BIST) for Optimized ALU.

B. Built-In Self-Test

Once BIST finds a fault, the readjustment in connections to exchange the faulty give a fault free one may be a style drawback and would be not be mentioned here.
The BIST techniques area unit classified supported the operational condition of the circuit below check (CUT):

1. Offline BIST

Deals with testing a system once it's not winding up its traditional functions (Test mode, Non-Real-Time error detection). Testing by exploitation either on-board TPG with Output Response analyzer (ORA) or small diagnostic routines. Structural is Execution supported the structure of the CUT (Explicit fault model - LFSR). Practical is running supported practical description of CUT (Functional fault model - Diagnostic software).

2. Online BIST

Testing occurs throughout traditional practical operational conditions (No check mode, Real- Time error detection).concurrent is occurs at the same time with traditional practical operation (realized by exploitation cryptography techniques). Non concurrent is
administrated whereas in idle state (Interruptible in any state, complete by death penalty diagnostic software/firmware routines).

C. Schematic Shot

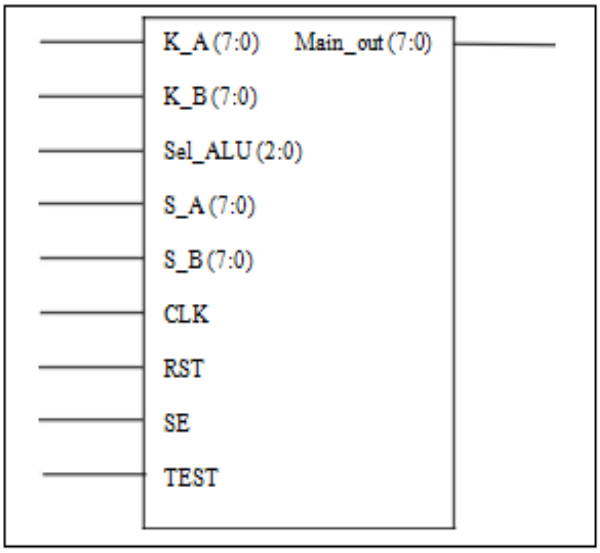

Fig.4. RTL for proposed secure cell design

It shows the schematic diagram for my proposed testing circuit. K is security key; sel is selection line for arithmetic and logical operation, S is scan in pin, CLK is clock signal, RST is reset, Test and SE is enable pin as 1. Then only execution gets starts.
After 8 bit key k assigned in the XOR gate, we started the process. Assign Test as 3 bit value 110, run the simulation process and get the output containing fault. It can mention as 4^{th} bit of main out contains 1 other bits are 0. Hence we concluded that this design has fault in that specific bit. It shows the accumulator output with fault determination.
After 8 bit key k assigned in the XOR gate, we started the process. Assign Test as 3 bit value 000, run the simulation process and get the output containing without fault. It can mention as all bit of main out contains 0 no bit has 1. Hence we concluded that this design has no fault in all 8 bit of main out. So we can go for hardware design. It shows the accumulator output without fault determination.

D. Algorithm

```
ALU

Main_8_Bit_Alu_F Logic Cone (
A (Cone_A_In),
B (Cone_B_In),
Sel (Sel_Alu),
Main_Out (Main_Out_Lc)  );

SECURE CELL

assign Sel= {Test, SE};
Dff Dff_Block (.Clk (Clk), .Rst (Rst), .D (Mux_Out), .Q (Out));
Mux_4X1 Mux_Block (.A(k),.B(Out),.C(Out),.D(SI),.Sel(Sel),.Out(Mux_Out));

Mux 4X1

always @ (A, B, C, D, Sel)
 begin
  case (Sel)
    2'b00: Out=A;
    2'b01: Out=B;
    2'b10: Out=C;
    2'b11: Out=D;
  end case
 end
```

Fig.5. Algorithm for proposed secure cell design

E. *Results*

When we assign the clock as rising edge is 1 and falling edge is 0. Then enable the test and SE pin as 1, start to assign input value for flip-flop. It gave the output for secure cell.

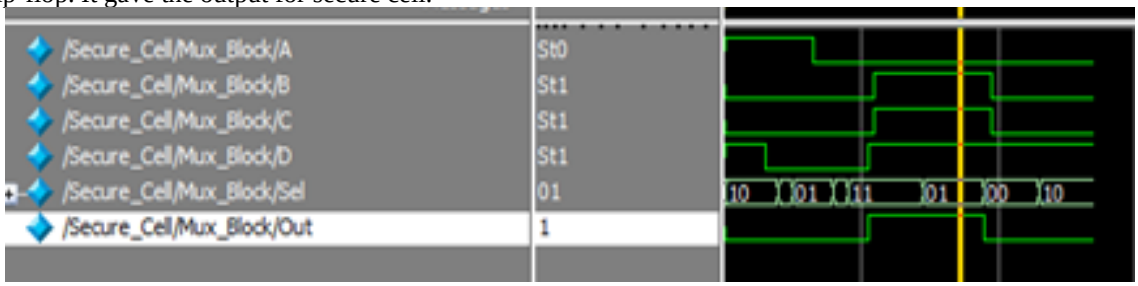

Fig.6. Behavioral simulation for multiplexer

V. CONCLUSION

We have proposed fresh frame work for secure cell architecture to test combinational circuit as accumulator (adder, subtractor, logic gates, etc). From our proposed design we can easily identify the fault in the specific bit of output through Verilog HDL code in simulation with Xilinx software. Hence we concluded that output bit contains binary number 1, it can consider as fault. If does not contains binary number 1 only having binary number 0 as shows in fig 8. We can say that it does not have any fault. This process is very easy to design, fabricate and manufacture the chip with fault free and prevent the leakage of key k.

FUTURE WORK

Numerous chips unavoidably have secondary passages as a piece of manufacture and testing process, yet they should be made as secure as conceivable to anticipate assaults. Planning for testing 40nm and 28nm chips is in progress. Assessment of items against new assaults growing new assault strategies and procedures. Maintaining delay time low, speed increasing and area over headed. Design and Test the sequential circuits with framework for security and fault free chips in future.

REFERENCES

1. Ujjwal Guin, Ziqi Zhou, And Adit Singh, "Robust Design-For-Security Architecture Forenabling Trust In Ic Manufacturing And Test," In *Proc.*IEEE Transactions On Very Large Scale Integration (Vlsi) Systems 1063-8210 © 2018 IEEE
2. Abdallatif S. Abu-Issa And Steven F. Quigley, "Bit-Swapping LFSR And Scan-Chain Ordering: A Novel Technique For Peak- And Average-Power Reduction In Scan-Based Bist," In Proc. IEEE Transactions on Computer-Aided Design Of Integrated Circuits And Systems, Vol. 28, No. 5, May 2009
3. Ahmad Al-Yamani, Narendra Devta-Prasanna, Erik Chmelar, Mikhail Grinchuk, Arun Gunda, "Scan Test Cost and Power Reduction Through Systematic Scan Reconfiguration," In Proc. IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems, Vol. 26, No. 5, May 2007
4. Shibaji Banerjee, Dipanwita Roy Chowdhury, "An Efficient Scan Tree Design For Compact Test Pattern Set," In Proc. Proceedings Of The 19th International Conference On Vlsi Design (Vlsid'06) 1063-9667/06 $20.00 © 2006 IEEE
5. Mitrajit Chatterjee And Dhiraj K. Pradhan, "A Bist Pattern Generator Design For Near- Perfect Fault Coverage," In Proc. IEEE Transactions On Computers, Vol. 52, No. 12, December 2003
6. Michal Filipek, Grzegorz Mrugalski, "Low-Power Programmable Prpg with Test Compression Capabilities," In Proc. IEEE Transactions on Very Large Scale Integration (Vlsi) Systems, 1063-8210 © 2014 IEEE
7. Zhou Jiang, Dong Xiang, "A Novel Scan Segmentation Design for Power Controllability and Reduction in At-Speed Test," In Proc. 2015 IEEE 24th Asian Test Symposium
8. Jinkyu Lee And Nur A. Touba, "Lfsr-Reseeding Scheme Achieving Low-Power Dissipation During Test," In Proc. IEEE Transactions On Computer-Aided Design of Integrated Circuits And Systems, Vol. 26, No. 2, February 2007
9. Xijiang Lin Janusz Rajski, "Adaptive Low Shift Power Test Pattern Generator For Logic Bist," 2010 19th IEEE Asian Test Symposium
10. Lei Li And Krishnendu Chakrabarty, "Test Set Embedding for Deterministic Bist Using a Reconfigurable Interconnection Network," In Proc. IEEE Transactions on Computer-Aided Design Of Integrated Circuits And Systems, Vol. 23, No. 9, September 2004
11. Mehrdad Nourani, Mohammad Tehranipoor, "Low-Transition Test Pattern Generation For Bist-Based Applications," In Proc. IEEE Transactions On Computers, Vol. 57, No. 3, March 2008
12. M. Omaria D. Rossi F. Fuzzi C. Metra, "Novel Approach To Reduce Power Droop during Scan-Based Logic Bis," In Proc. 2013 18th IEEE European Test Symposium (Ets)
13. U. Guin, Z. Zhou, And A. Singh, "A Novel Design-For-Security (Dfs) Architecture To Prevent Unauthorized Ic Overproduction," In Proc. IEEE Vlsi Test Symp. (Vts), Apr. 2017, Pp. 1–6.
14. U. Guin, K. Huang, D. Dimase, J. M. Carulli, M. Tehranipoor, And Y.Makris, "Counterfeit Integrated Circuits: A Rising Threat In The Global Semiconductor Supply Chain," Proc. IEEE, Vol. 102, No. 8,Pp. 1207–1228, Aug. 2014.
15. U. Guin, D. Dimase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, And The Challenges Ahead," J. Electron. Test. Vol.30,No.1,Pp.9–23,2014
16. Rigui Zhou, Yancheng Li, Manqun Zhang, Benqiong Hu. "Novel Design For Reversible Arithmetic Logic Unit", International Journal of Theoretical Physics, 2014.
17. Filipek, Michal, Grzegorz Mrugalski, Nilanjan Mukherjee, Benoit Nadeau-Dostie, Janusz Rajski, Jedrzej Solecki And Jerzy Tyszer. "Low-Power Programmable Prpg with Test Compression Capabilities", IEEE Transactions on Very Large Scale Integration (Vlsi) Systems, 2015.
18. K.N.Devika, Ramesh Bhakthavatchalu. "Design of Efficient Programmable Test-Per-Scan Logic Bist Modules", 2017 International Conference on Microelectronic Devices, Circuits and Systems (Icmdcs), 2017.
19. P Dhanesh, A Jayanth Balaji. "Dual Threshold Bit-Swapping Lfsr For Power Reduction In Bist", 2015 International Conference on Advanced Computing and Communication Systems.
20. John L. Hennessy, David A. Patterson. "Arithmetic For Computers",Elsevier Bv, 1994.
21. Jose M.Solana. "Reducing Test Application Time, Test Data Volume and Test Power through Virtual Chain Partition", Integration, 2009.
22. Irith Pomeranz, Sudhakar M.Reddy. "On The Switching Activity In Faculty Circuits During Test Application", 2016 IEEE 25th Asian Test Symposium (Ats).
23. Wang, Weizheng, Shup Cai, And Lingyun Xiang. "Reducing Test Power and Improving Test Effectivness For Logic Bist", Jsts Journal of Semiconductor Technology on Science, 2014.