International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Area Efficient Design of BIST Technique in UART using Circuit under Test (CUT)

Bandike. Dinesh Kumar, D. Jayanthi, N. Arun Vignesh, K. Jamal

Abstract: ***Multiplication float of IC exchange, numerous microchips are demonstrated in a foundry. The nearness of carrying on inbuilt equipment Trojans (HTs) is of tight security worry, without the attention to end clients or unique originators of a host, to distinguish sans trojans circuit. For this creator looks for low exchanging likelihood nets to embed HTs to lessen control spillage. However, the circuit's net encounters a particular state and turning probabilities on test and capacity mode. The proposed strategy, quick heuristic, is incited on circuit under test (CUT). This is an insignificant mind-boggling, high exact, famous standard and complex circuit tried with sensible deferral. In equipment self-testing, (worked in individual test) offer a commendable answer for lessens item disappointment, intricacy happens in multiplication. Plan and incitation of all-inclusive offbeat collector transmitter (UART), to diminish control, territory, to arrive at convenient, steady and dependable information transmission is utilized.***

Keywords: Hardware Trojan (HT), state transition, universal asynchronous and synchronous receiver transmitter (UART) built-in-self-test (BIST)

I. INTRODUCTION

Integrated Circuits (IC) requires more security because, in IC fabrication process test services, designs and tools are given from outside. These outside people are considered as third parties, apart from third parties, untrusted people existence may present in IC design flow. So addition of extra logic modifies the internal circuit, these malicious modifications are considered as hardware trojans. Presence of hardware trojan IC violates its specifications and it doesn't produce correct output. So, IC has lost its functionality. So, attacker or adversary has more number of chances to add malicious logic to internal circuit of IC from outside. Hardware trojan is confined in IC, triggering circuit is either analog circuit or digital circuit. Attacker can design trojan trigger activation at very rare occurring internal node conditions of IC. These rarely occurring sequences cannot be captured by Attacker can introduce malicious function by insert more number of trojans of different forms and sizes. Trojan leaks data from side channel, it is considered as multilevel attack and encryption key may leak during this attack.

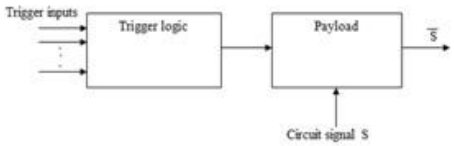


Fig :1 Block diagram of hardware trojan

Based on the type of activation, Trojans are classified as, combinational and sequential Trojan as in Fig: 1(a) and 1(b) respectively. Combinational Trojan uses combinational circuits such as AND gate, comparator and multiplexers for triggering purpose.

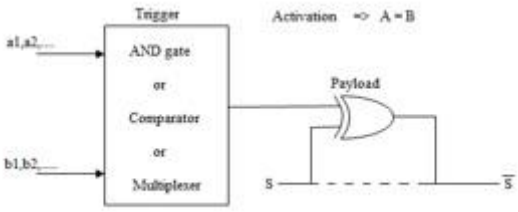


Fig: 1(a) Combinational Trojan

Describes a sequential trojan which uses sequential circuit such as counters for triggering

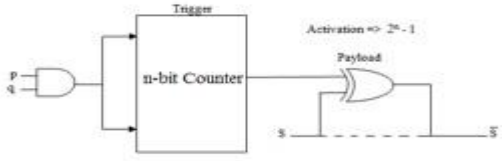


Fig: 1(b) Sequential Trojan

Ratanpa G.B.et al[2014] has implemented cryptographic algorithms to extract secret data.

Manuscript published on January 30, 2020.
* Correspondence Author
Bandike. Dinesh kumar*, Mtech student, department of ECE, Gokaraju Rangaraju Institute of Engineering and Technology. Hyderabad, TS, India. Email: dineshweb2010@gmail.com
Dr. D. Jayanthi, Ph.D Degree, Department of Electronics and Communication engineering,Anna University, Chennai, TN, India Email:jayanthivlsi@gmail.com
Dr. N. ArunVignesh Assoc. Professor, Department of Electronics and Telecommunication Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad , India Email:arunvignesh44@gmail.com
K. Jamal Assoc. Professor, Department of Electronics and Telecommunication Engineering Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India Email:kjamal24@gmail.com

Differential power analysis (investigation) (DPA) and simple power analysis (SPA) attacks analyst the equipment control consumption. This countermeasure significantly increases this DPA undertake the power trace samples. The countermeasure does not require any assumptions about the design of the hardware under protection.

X.Cui and K.Ma et al[2014] has executed plan rules to help run-time trojan and quick recuperation by investigating assorted variety of untrusted outsider IP centers. With these plan rules, we show the streamlining way to deal with limit the expense of usage as far as the quantity of various IP centers.

Swarup Bhunia et al[2014] analyses the different forms of hardware trojan attacks counter measures. By using logic testing and side channel analyses trojan detection is a described. Trojan prevention by obfuscation method and layout filler approaches is explained. To enhance an IC security, some design approaches are described.

J.li and J. Lach et al[2008] proposed an exact estimating of IC that can be utilized to give the ideal conformation and structure modification location. This ease the primary IC usefulness and can be performed at-speed at both test-time and run-time.

Miron Abramovici et al[2009] proposed a defense logic to detect tampering attacks. The security monitors in this technique perform online checking to identify hardware trojans in the IC without golden chip reference. The logic function of this technique is invisible so reverse engineering is not possible.

J.Yin et al [2009] has tried strategies usage of eight particular assault procedures register transfer level (RTL) equipment trojans to fix the security of an alpha encryption module.

M. Tehranipoor et al[2009] has developed a detailed overview and analysis of the current state of knowledge in design that impact the functionality or transmit key information to the adversary. Such malicious circuits are known as trojans.

H. Salmani et al[2011] proposed a method to decrease the activation time of trojan. This paper describes time to generation of transition in trojans. Transition is computed by using geometrical distribution and estimation of number of clock cycles required to generate a transition. Insertion dummy scan flip-flop reduce the generation time of transition. This paper describes dummy flip-flop insertion is an s38417 benchmark

A Waksman et al[2013] proposed FANCI tool to detect suspicious wires in the design, these wires can carry trigger signals. Suspicious wires affect intermediate outputs, so truth tables are implemented for intermediate outputs. Which describes within design how wires influence other wires. FANCI tool detected triggers in 18 trust hub benchmarks.

J. Rajendran et al[2010] has implemented concurrent error detection (CED) techniques to detect error outputs generated by trojans and using a 3PIP vendors and operation-to-3PIP to-vendor allocation constraints between 3PIPs from the same vendor.

II. EXISTING WORK

Basically, HT is a deadly disease introduced into the circuit at some point of fabrication in an unreliable industry. Presence of HT results in severe safety leakage of the system. So as to conquer this, it's far and utmost crucial to perceive or come across whether or not a circuit carries HT or no longer. Right here, we stumble upon two (2) phrases: (a) Nests with extreme state probabilities - which are nothing but extreme or active nets. (b) Nests with low switching probabilities - which are nothing but inactive nets. As a solution to triggering of HT: (a) HT designers use nets with extreme state probabilities in order to create states with such an uncommon mixture's (b) HT designers use nets which devour low power on switching from one state to some other in order now not to stumble upon the leakage strength problems.

A secretly-inserted circuit typically operates in two modes: (a) Dormant mode (inactive) (b) Triggered mode (active) There are certain symptoms to distinguish these two modes. They are: (a) Dormant mode (inactive): Power and delay are too small and can be neglected and hence causes a minute or even may not cause any harm to the circuit. (b) Triggered mode (active): This causes adverse effects which may include

i. Varied Outputs.
ii. Negative Effects on performance.
iii. leak confidential records

Present day techniques to perceive HT are

(a) Online detection
(b) Offline detection

These both detections are followed by recovery

(a) Online detection: Evolves confined a guideline to model and restrict the design and fabrication process. The exploited restrict assist increase the feasibility of detecting the interest of HTs at run-time and recovering the host circuits from peculiar states.

(b) Offline detection: Tries to perceive if a fabricated chip includes any HTs at the test phase section earlier than the chip's deployment. Both strategies have their pros and cons. Evaluating to Online detection, offline detections have considerable sources in terms of time and detection techniques, but need to locate the secret triggering system set through[7] HT designers. Thinking about the almost unlimited design space of HT triggering system, this will be one of the most difficult obligations. Once in a while HT triggering might be by chance carried out which leads to energy evaluation. To reduce this, it is better to opt for extreme nets (inactive nets) or for the nets that hardly switch for the designed triggering component.

As we already came across the term probability, this is also of two types:

(a) State probability (b) Switching probability There is a lot of difference between the two probabilities. A state probability is to obtain the next states based on probability calculations. Switching probability switches between on or off states based on probability calculations.

Again, these two probabilities operate in two modes:(a)Test mode (b) Function mode Nests with low activeness on Test and Function mode are more preferable[2]. First, nets with low activeness and extreme nets on function mode are to be found.

A sensible decision of HT fashioners is to search for the nets with low liveliness on both test and capacity mode. This is done by using State transition defined by FSM of CUT. Keeping in view the points and implementing them in a circuit is an example shown in Fig: 2 Hardware Trojan and its host circuit. The circuit consists of two (2) sections. One of them is the secretly inserted circuit and the other is the host circuit.

The nets of the host (right here G4 and G5) are decided on with the aid of HT to layout its trigger part. To begin with preset is performed ({G4, G5} is 00), this is analyzed by HT. Now HT is activated to alter the host function i.e.., G6- state is altered.

It is very often assumed that if a HT desires to conceal from attack based on information gained from the implementation analysis, it would be better to pick out the nets that do not easily switch (referred to as inactive nets there after) to reduce the count of the nets that

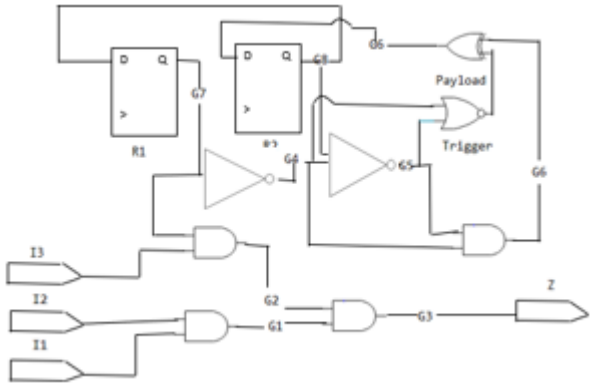


Fig:2 Hardware Trojans of CUT (Circuit under test)

Remains in the same state of longer duration of time (referred to as extreme nets thereafter). Here switching probabilities are computed with an aim to detect the inactive nets. All the bits of the inputs and registers are set/reset (0 or 1) which enables to drive switching probabilities of all the nets in CUT. Here we across a term “Best Candidate” which makes the sense as most suitable. To activate HT, inactive nets are the best candidates. During the phase of circuit testing, addition of spare control. flip-flops is done to nets to enable manual rise of switching probabilities, with a scope to increase the power consumption of HT. This is a method in which setting of cut to test and all the primary inputs and flip-flops in a random manner and the cut changes from one state to other state randomly.

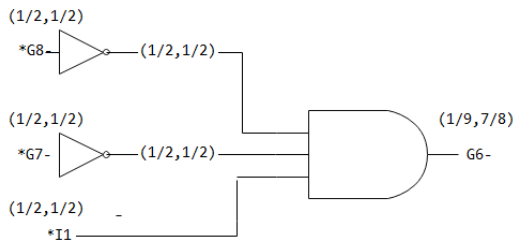


Fig:3 Cone of the Nets

The idle nets are considered as the best contender for the activating sign of HTs, as per . Extra control flip-flops are then added to these nets to physically bring their exchanging probabilities up in the period of circuit testing, with the would like to build the power expending of HT's. In this technique, the CUT is set to test mode[6], and all the essential sources of info and flip-flops are set arbitrarily and the CUT travels between irregular states.

It is critical to take note of that, in any case, a HT can be incidentally activated on capacity mode too, i.e., a HT is activated in the field however not in the setting wanted by the Trojan planner. For instance, most mission-basic applications will have numerous preliminary tasks performed routinely before their official missions.

Taking for the benefit of HT architects, unintentional activating at preliminary tasks, where hosts are on capacity mode does not satisfy their vindictive missions but rather just demolishes their organizations and notorieties, and subsequently ought to be stayed away from as much as being coincidentally activated and control spillage on test mode. Along these lines, a sensible decision for HT architects is to search for the nets with low liveliness on both test mode and capacity mode.

Contrasting with the current works that search for the nets with low liveliness on test mode, this paper will search for the nets that are inert on work mode[4], i.e., by considering the real state advances characterized by the limited state machine (FSM) of the CUT. Also, we accept that the crossing point of nets with low liveliness found on the two modes are the "best applicants" supported by the HT planners. The commitments of this paper are abridged underneath.

- Here the simulation table contains the test mode estimation and function mode simulation, we have calculate with help of state and switching probability
- There are some formulation of calculation needed to verify the results

1. n P(i = 1), the probability of net i begin 1.
2. b P(i = 0), the probability of net i begin 0.
3. Pt(i), the switching probability of net i.
4. A total-state represent of the circumstance of receiving a certain input pattern

		Test-mode Estimation	Function-mode Simulation
G1	P(G1=1)	0.2500	0.2500
	P(G1=0)	0.7500	0.7500
	Pt(G1)	0.1875	0.1878
G2	P(G2=1)	0.2500	0.1248
	P(G2=0)	0.7500	0.8752
	Pt(G2)	0.1875	0.1248

G3	P(G3=1)	0.0313	0.0306
	P(G3=0)	0.9688	0.9694
	Pt(G3)	0.0313	0.0306
G4	P(G4=1)	0.7500	0.7503
	P(G4=0)	0.2500	0.2497
	Pt(G4)	0.2500	0.2497
G5	P(G5=1)	0.7500	0.7503
	P(G5=0)	0.2500	0.2497
	Pt(G5)	0.2500	0.2497
G6	P(G6=1)	0.2500	0.2497
	P(G6=0)	0.7500	0.7503
	Pt(G6)	0.2500	0.2497

Table I: Simulation Results

- The equation to be calculate the state probabilities of output 0 of a 2-inputs AND gate whose input are A and B have to be calculate only in one step

$$P(0 =1) = P(A = 1)* P(B = 1) \quad 2.1$$

$$P(0 = 0) =1 – P(0 = 1). \quad 2.2$$

- The switching probability of the output should be calculated and verified whose input A and B in two steps there are

$$P(0 =1) = P(A = 1)*P(B = 1) \quad 2.3$$

$$P(0 = 0) = 1 -P(0 =1). \quad 2.4$$

$$Pt(0) = P(0 = 0)*P(0 =1) \quad 2.5$$

III. PROPOSED WORK

Taking this approach to the next level from CUT to BIST and implementing BIST in UART forms the central part of this paper[1]. However, emphasizes additionally on data exchange at excessive speed protocol utilization within it using Field programmable gate array (FPGA) era. Least squares and modules are utilized to structure this UART to diminish the testing multifaceted nature. Structured UART shows that the quantity of sign or image changes that happen every second is 4 Mbps, which is manufactured into a solitary chip. The quantity of bits that are conveyed per unit of time is just 0.00007. This system can be verilog HDL which is the system coding and proposed, examined and assessed using the ISE 6.0 tool of Xilinx and Verilogger Pro 6.5. For the layout implementation the Xilinx Spartan-2 FPGA (XC2S150) is used.

The technique implementation method of the network , circuit schematic and simulation outcomes could be mentioned in essence inside the following sections. This UART satisfies the device needs of high integration, the reduction in the rate at which error occurs in the transmission of data and at low value. This UART structure operates in two different modes. Initially is the BIST mode where the UART does the self testing. The other is normal mode. In normal mode, the device works like the one which does neither transmits nor receives the data at the same time(irrespective of the clock).

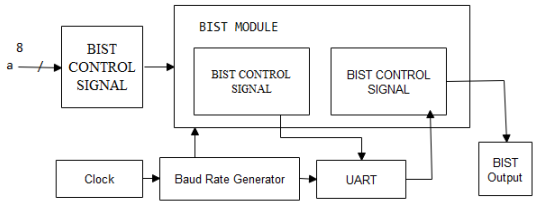


Fig: Area Efficiency of UART structure

Propose project work illustrates security architecture, it is capable to protect any application bits and malicious attacks. This application is carry out with proposed security technique ensures secured and accurate operations. Integrated Circuit (IC) development process has several number stages. Because of some modification in the design, IC gives undesired functionality and generates incorrect outputs. These malicious modifications are referred ad hardware Trojans, So this applications of BIST is consider as a security is must. Proposed security technique detects the hardware Trojans during run time.

The block diagram contains the BIST module application here this BIST control signal contains the input of an signal it consists of the eight bits has input it passing through the BIST module. Here the Module has two block contains as Random Pattern Generator and Received Bit Analyzer. An other part contains the clock through Baud Rate Generator it goes through the Universal Asynchronous Receiver Transmitter (UART), passing the output of an BIST output. Let us consider existing work about UART and BIST how it happens in each block and to know about hardware trojan attacks and how applications was taken in each step, Now let us discusses about existing work.

- **Random Pattern Generator:** Irregular Pattern Generator (RPG)generates arbitrary examples which can be utilized for the check of gadget like UART. The RPG is a piece of the BIST in the check of the circuits. Numerous strategies have been proposed for the BIST hardware plan. To create bytes to test the circuit the strategy for an irregular example generator (RPG) is utilized. Every one of these bytes are utilized straightforwardly in the CUT to get better shortcoming inclusion. A got bit analyzer assesses the reaction of the CUT with these bytes.
- **Received Bit Analyzer:** This is a comparator which is utilized to look at the got and transmitted piece design. And after that it gives the estimation of bit blunder rate
- **Baud Rate Generator:** Baud rate is mainly used to measure the transfer data rate. Most CUT chips have a built in buffer of anywhere
- The UART module incorporates a committed 16-piece baud rate generator with a Presale. The UxBRG register controls the hour of a free-running 16-piece clock:

$$Baud_{Rate} = \frac{Fcy}{16.(UxBRG+1)} \quad 3.1$$

The value of the UxBRG register for a specified baud rate is given by

$$UxBRG = \frac{Fcy}{16.Baud\_Rate} - 1 \quad 3.2$$

3.1 BIST Module

Worked with Built In Self-Test (BIST) has risen as a promising answer for the VLSI testing issues. BIST is a DFT technique is ought to be planned for distinguishing defective segments in a framework by fusing the testing rationale on a chip.[9] The BIST is notable for its various points of interest, for example, improved testability, at-speed testing and decreased the requirement for programmed test gear (ATE).In BIST, a straight criticism move register (LFSR) creates test designs and different info move register MISR) compacts test reactions.[5] Test vectors applied to a circuit under test at apparent working repeat may have progressively typical or possibly top power dispersal than those in standard mode.
The clarification is that the subjective thought of models reduces the connection between the pseudorandom plans created by LFSR appeared differently about common utilitarian vectors. It realizes all the more trading and power dispersal in test mode. BIST is a structure for testability (DFT) procedure in which testing is finished using worked in gear features.[3]

Since testing is consolidated with the gear, it is snappier and beneficial BIST configuration showed up in fig.3.1 needs three additional hardware squares, for instance, a model generator, a For plan generators, we can use either a ROM with taking care of models or a counter or an immediate information move register (LFSR).

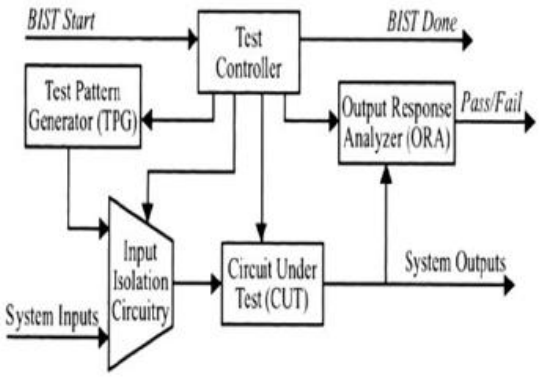
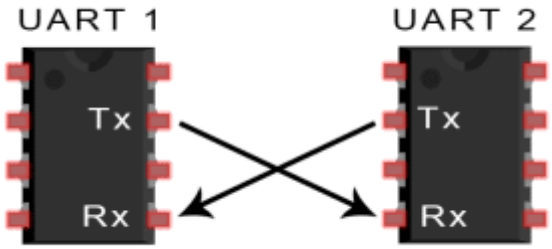


Fig:3.1 BIST basic block diagram

3.2 UART(Universal asynchronous receiver transmitter)

In UART correspondence, two UARTs discuss straightforwardly with one another. The transmitting UART changes over parallel information from a controlling gadget like a CPU into the sequential structure transmits it in sequential to the accepting UART, which at that point changes over the sequential information once again into parallel information for the getting gadget. Just two wires are expected to transmit information between two UARTs. Information streams from the Tx stick of the transmitting UART to the Rx stick of the getting UART



UARTs transmit information non concurrently, which implies there is no clock sign to synchronize the yield of bits from the transmitting UART to the examining of bits by the accepting UART. Rather than a clock signal, the transmitting UART adds begin and stop bits to the information parcel being moved. These bits characterize the start and end of the information parcel so the accepting UART realizes when to begin perusing the bits.
At the point when the accepting UART identifies a beginning piece, it begins to peruse the approaching bits at a particular recurrence known as the baud rate. Baud rate is a proportion of the speed of information move, communicated in bits every second (bps). Both UARTs must work at about a similar baud rate.

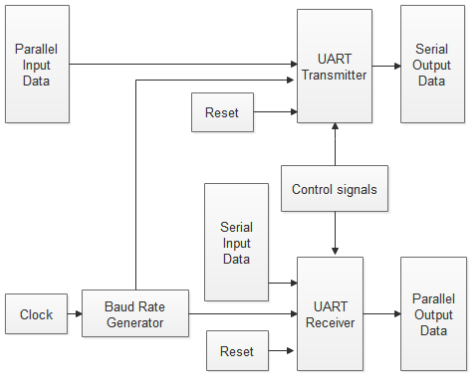


Fig: 3.2 UART Structure

3.3 UART Transmitter and Receiver

3.3.1 Transmitter

The reworked state machine outline of the plan transmitter. Here transmitter is addressed by 3 states. At whatever point 'reset' is '1' 'enable' is '0''tx_reg' is '0' 'tx empty' is '1' the transmitter is in the "Start" state. A 'start bit' is insisted when 'reset' is '0' 'enable' is '1' 'tx reg' is '1' 'tx unfilled' is '0'. Resulting in delegating the 'start bit' the "Move" state will be started. This state works till 'Last data bit'. Exactly when the 'Last data bit' is moved, the "Stop" state begins. In this express, the 'stop bit' is expressed. Starting there ahead, the state machine switches back to the "Start" state and confirms another 'start bit' for another edge.

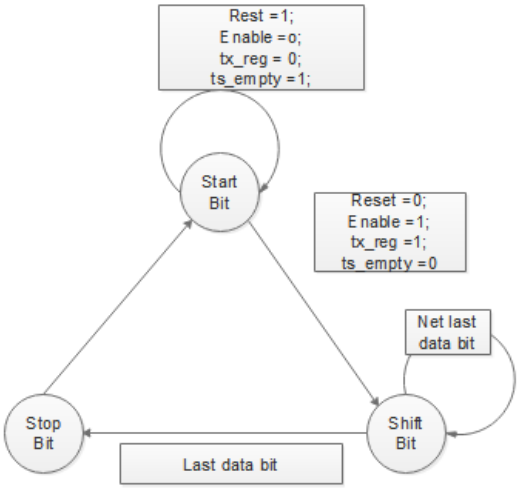


Fig:3.3.1 Transmitter State machine

3.3.2 Receiver

The states machine of the beneficiary with 3 states. At whatever point 'engage' is '0'; 'rst n' is '1'; 'ready_in' is'0'; 'ack_out' is '1', the authority state machine is in the "OFF state", i.e., no data bit is gotten. At whatever point 'engage' is '1'; 'rst_n'is '0'; 'ready_in' is '1'; 'ack_out' is '0', the "Move state" begins. This state works till the 'Last data bit'. Right when the 'Last data bit' is moved, the "Hold and Go" state begins. The state machine returns to the "Move state" and trusts that another packaging will be moved. At whatever point 'engage' is '0'; 'rst_n' is '1'; 'ready_in' is'0'; 'ack_out' is '1', the beneficiary state machine switches back to the "OFF state".

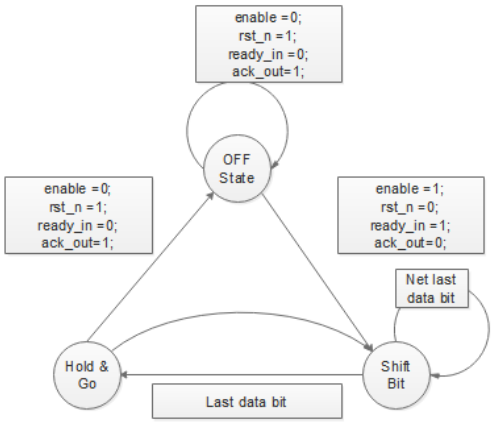


Fig:3.3.2 Receiver State machine

3.4 USRT(universal synchronous receiver transmitter)

The USART's synchronous capacities were principally planned to help synchronous conventions like IBM's synchronous transmit-get (STR), double synchronous interchanges (BSC), synchronous information interface control (SDLC), and the ISO-standard significant level information connect control (HDLC) synchronous connection layer conventions, which were utilized with synchronous voice-recurrence modems. These conventions were intended to utilize transfer speed when modems were simple gadgets. On those occasions, the quickest offbeat voice-band modem could accomplish all things considered paces of 300 pieces/s utilizing recurrence move keying (FSK) balance, while synchronous modems could run at speeds up to 9600 pieces/s utilizing stage move keying (PSK). Synchronous transmission utilized just marginally over 80% of the transfer speed of the now progressively recognizable nonconcurrent transmission, since the start and stop bits were superfluous.

Those modems are out of date, having been supplanted by modems that convert offbeat information to synchronous structures, however, comparable synchronous media communications conventions get by in various square situated advances, for example, the generally utilized IEEE 802.2 (Ethernet) interface level convention. USARTs are still here and there incorporated with MCUs. USARTs are as yet utilized in switches that interface with outside CSU/DSU gadgets, and they regularly use either Cisco's exclusive HDLC execution or the IETF standard point-to-point convention (PPP) in HDLC-like confining as characterized in RFC 1662.

3.4.1 Operations of Usrt

The activity of a USART is personally identified with the different conventions; allude to those pages for subtleties. This area just gives a couple of general notes.

1. USARTs in synchronous mode transmits information in outlines. In the synchronous activity, characters must be given on time until an edge is finished; if the controlling processor doesn't do as such, this is an "underrun mistake," and transmission of the edge is prematurely ended.
2. USARTs working as synchronous gadgets utilized either character-situated or bit-arranged mode. In character (STR and BSC) modes, the gadget depended on specific characters to characterize outline limits; in bit (HDLC and SDLC) modes prior gadgets depended on physical-layer signals, while later gadgets assumed control over the physical-layer acknowledgment of bit designs.
3. The asynchronous line is rarely quiet; when the modem is transmitting, information is streaming. At the point when the physical layer demonstrates that the modem is dynamic, a USART will send a constant flow of cushioning, either characters orbits as suitable to the gadget and convention.

IV. RESULTS

5..1 Existing work Simulation results

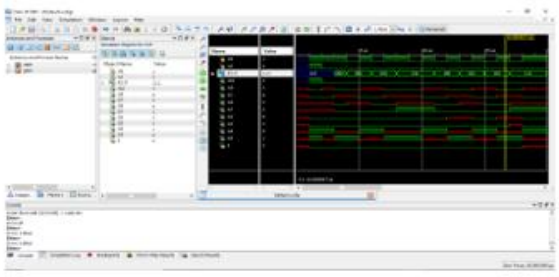


Fig 5.1 Existing Work Simulation results

- Inputs are clk, rst, and I [3:0] and input encoded parity bits G1-G7 are the outputs of rtst .If the rst is 1 then, output is reste to 0, and it should make make reset values by giving vales rst =1 and clk = 0 , so it will reset the system

- Wile doing all because if we don with reset the values the will posedage values it will initial values to get started we taking rst =1 anc clk = 0.
- When we given clk = 0 over inputs values will be taken due to posedage
- Now after completing each steps we should give inputs values as bits types like 000,001,010,011,100.101,110,111.
- While given this inputs each bits we should give clk = 1 and run the simulations and next step we should make clk = 0 for posedage.

5.2RTL Schematic of the design

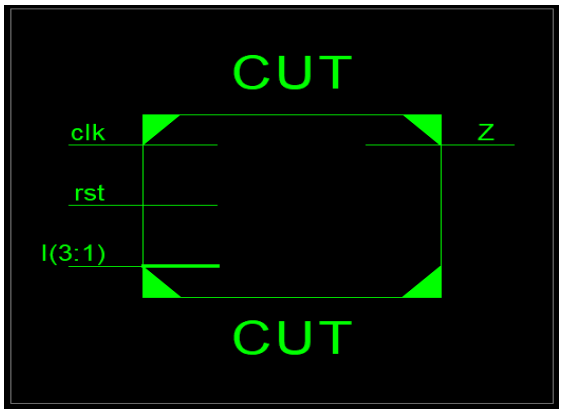


Fig:5.2.1 Schematic of the design

The overall schematic of the design is as shown in fig.5.1.2, the schematic is a block level representation of the design with logic interconnections and primary inputs/output ports

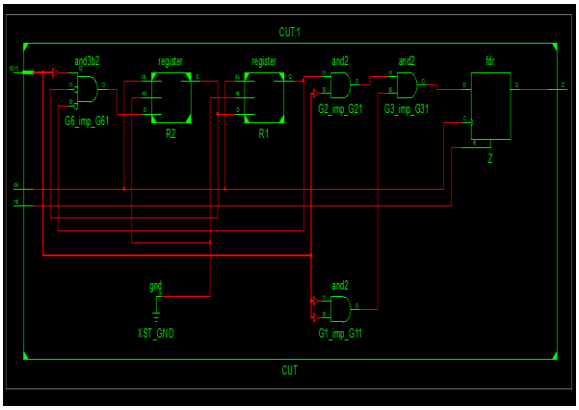


Fig:5.2.2 Schematic data selector

- The data-selector circuit schematic is as shown in Fig: 5.1.3; it performs data selection as specified by the register to the CUT.
- This selection of type of architecture based on number of input samples used in determined by this circuit.
- The circuit shown in Fig: 5.4 schematic view two register, has activation signal that will generating signal which is passing from registers to flipflops ang generate the internal cut proposing of an output.

5.3Proposed work Simulation results

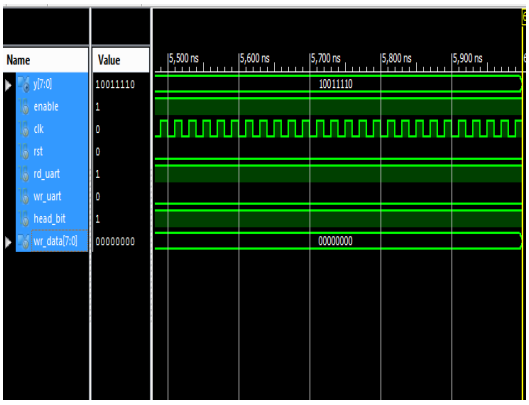


Fig:5.3 Proposed work results LFSR

- This low power LFSR(Linear feedback shift register), we used this lfsr for shifting the values ‘0s’ ‘1s’ by interchange values and gones randomly change one by one proposing
- Here taken by y[7:0] bits that has inputs bist control signal and read uart and write uart to inputs was taken because with should read and write the inputs values .

5.4RTL LSFR

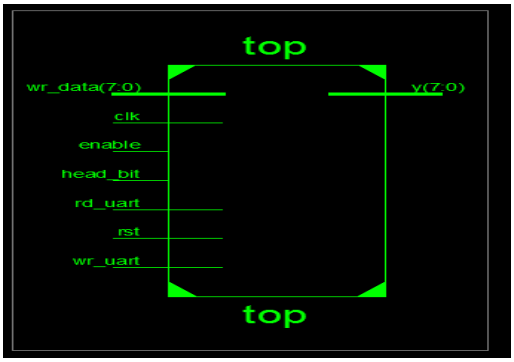


Fig:5.4 RTL view of an design

- The Fig: 5.4 shows an schematic view of an design has I[7:0] inputs and y[7:0] this design show each block representation of the designs with logic designs
- The Fig: 5.4 shows internal diagram of LFSR schematic, there internals inputs are BIST and UART show in control top model block.

Table Ii Design & Summary Of Lfsr

Device Utilization Summary (Estimated values)			
Logic Utilization	Used	Available	Utilization
Number of slices	42	4656	0%
Number of slice flipflops	59	9312	0%
Number of 4 input LUTs	68	9312	0%
Number of bonded IOBs	16	232	6%
Number of GCLKS	2	24	8%

Synthesis Report of LSFR: The proposed method is simulated in Xilinx 14.4 ISE to verify the logic using Verilog hardware description language (VHDL) and a test bench is created to test the logic. Here available slices are 4356, but its takes only 42, like this the area will be reduced compared to normal low power Linear Feedback shift register (LP-LFSR) and also takes only 0% utilization. Here compared to CUT and normal LFSR is better.

5.5 RTL Low power LFSR

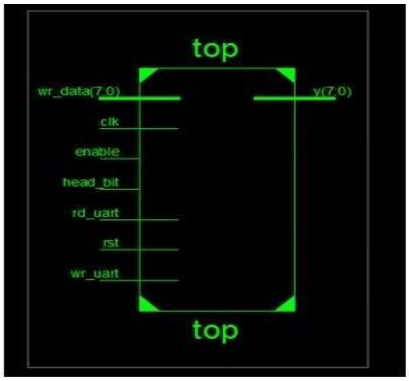


Fig 5.5 RTL Schematic design

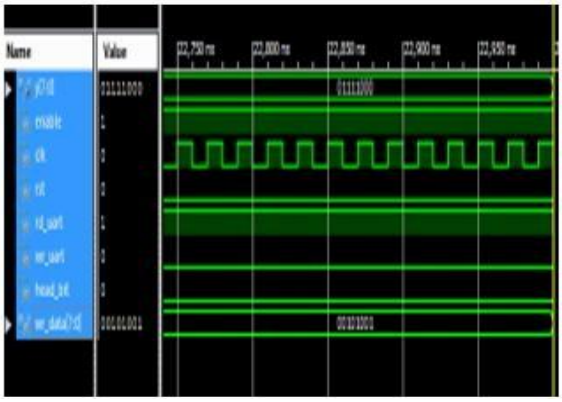


Fig:5.6 Simulation results of LP-LFSR

Table Iii Design & Summary Of Lp-Lfsr

Device Utilization Summary (Estimated values)			
Logic Utilization	Used	Available	Utilization
Number of slices	35	4656	0%
Number of slice flipflops	49	9312	0%
Number of 4 input LUTs	63	9312	0%
Number of bonded IOBs	16	232	6%
Number of GCLKS	2	24	8%

Synthesis Report of Low-Power LFSR: The proposed method is simulated in Xilinx 14.4 ISE to verify the logic using Verilog hardware description language (VHDL) and a test bench is created to test the logic. Here available slices are 4356, but its takes only 35 like, this the area will be reduced compared to normal low power Linear Feedback shift register (LP-LFSR) and also takes only 0% utilization. Here compared to CUT and normal LFSR is better.

V. CONCLUSION

This proposes novel method to identify the low activeness of nets on cut in its function mode. State and switching probabilities form the basis for the estimation of activeness of a net. The proposed method forms its basis on the transitions of state of the cut which offers best performance. Drawn from the experimental outcomes acquired from the popular benchmark suite and large-sized circuits on a proposed method: 1)With the high accuracy and efficiency calculates the state and switching probabilities of the nets of CUT

2) A net's experiencing state and switching probabilities are different in both function and test mode.

As the HT detection techniques advances, so the HT designs techniques. In this paper FPGA based implementation of UART with BIST capability is presented. Here all the modules are designed and simulated with Verilog HDL. Then the designed system is Xilinx Spartan-2 FPGA (XC2S150). A high-speed serial data transmitter transmits data at the rate of one bit each 0.25us which means the baud rate of 4 Mbps. The RS-422 communication standard is also tested and the bit error rate is only about 0.000007. This UART is much more flexible, speedy, low cost, and stable with respect to conventional one.

ACKNOWLEDGMENT

The authors would like to thank the authors, Dr. N Swetha, Head of department, Department of Electronics and communication engineering, GokarajuRangaraju Institute of Engineering and technology, Hyderabad and Dr. E.Logasanmugam, professor and Director, Sathyabama Institute of Science and technology.

REFERENCES

1. Minhui Zou and Xiantong Cui "Potential Trigger Detection for Hardware Trojans" IEEE Transcations on computer aided design of integrated circuits and systems, vol. 37, no 7, pp 1384-1395, JULY 2018
2. Nandeesha Veeranna and Benjamin Carrion Schafer " Hardware Trojan Avoidance and Detection for Dynamically Re-configuarable FPGAs" 2016 International Conference on Field Programmable Technology (FPT) Dec 2016, pp. 1-4.
3. Jamal, K., Chari, K. M., & Srihari, P. (2019). Test Pattern Generation using Thermometer Code Counter in TPC Technique for BIST Implementation. Microprocessors and Microsystems
4. Jiliang Zhang "A Practical Logic Obfuscation Technique for Hardware Security." IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 24, NO. 3, MARCH 2016, pp. 1193-1197.
5. K.Jamal, Dr.P.Srihari "Low Power TPC using BSLFSR" International Journal of Engineering and Technology (IJET), Vol 8 No 2 Apr-May 2016. Page no.759.
6. N. Fern, S. Kulkarni, and K. T. T. Cheng. "Hardware Trojans hidden in RTL don't cares Automated insertion and prevention methodologies". Test Conference (ITC), IEEE International, Dec.2015, pp. 1-8.
7. K. Xiao, D. Forte, and M. Tehranipoor, "A novel built-in self authentication technique to prevent inserting hardware Trojans," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 33, no. 12, Dec. 2014,pp. 1778–1791.
8. Swarup Bhunia, "Hardware Trojan Attacks: Threat Analysis and Countermeasures". Proceedings of IEEE, vol.2, no.8, Aug 2014, pp. 1229-1247.

9. K. Jamal, P. Srihari, K. Manjunatha Chari, B. Sabitha "Low Power Test Pattern Generation Using Test-Per-Scan Technique for BIST Implementation "ARPN Journal of Engineering and Applied Sciences
10. A. N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, "Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 33,no. 12, Dec. 2014 pp. 1792–1805.
11. M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," Proceedings of the IEEE, vol. 102, no. 8, pp. 1283–1295, 2014.
12. A. Waksman, M. Suozzo, and S. Sethumadhavan, "FANCI: Identification of stealthy malicious logic using Boolean functional analysis," Proceedings of the ACM Computer and Communications Security'13(CCS'13), Berlin, Germany, Nov. 2013, pp. 697–708.
13. Sheng Wei and Miodrag Potkonjak "Scalable Hardware Trojan Diagnosis" IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 20, NO. 6, JUNE 2012, pp. 1049-1057.
14. K.Jamal, Dr.P.Srihari, G Kanakasri "Test Vector Generation using Genetic Algorithm for Fault Tolerant Systems"International Journal of Control Theoryand Applications (IJCTA), 9(12), 2016
15. D.Jayanthi "Improving the performance of quality of Service parameters Using Mobile Node Positioning Algorithm in WLAN"vol 10,05 2018.
16. H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware Trojan detection and reducing Trojan activation time," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20,no. 1, Jan. 2012, pp. 112–125.
17. Huafeng Liu and Hongei Luo, LiweiWang "Design of Hardware Trojan Horse Based on Counter" International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, June 2011, pp. 1-3.
18. A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC piracy using reconfigurable logic barriers," IEEE Des. Test Comput. vol. 27, no. 1, Jan./Feb. 2010 ,pp. 66–75.
19. M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," Proceedings of the 46th ACM/IEEE Design Automation'09 (DAC'09) conference, San Francisco, CA, USA, Jul. 2009, pp. 688–693.
20. M. Abramovici and P. Bradley, "Integrated circuit security: New threats and solutions," Article No.55, Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research'09 (CSIIRW'09), Knoxville, TENNESSEE, USA, Apr.2009, pp. 1–3.

AUTHORS PROFILE

Bandike Dinesh kumar Completed B.Tech in ECE from JNTU Hyderabad in year 2017 and M.Tech in VLSI at Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, TS, India

Dr.D.Jayanthi received the BE Degree from Periyar Maniammai College of Engineering for Women in 1993, Mtech VLSI Design from sastra university in 2002. She obtained her PhD degree in VLSI Design from Anna University Chennai in 2013. She earned 22 years of teaching experience from various institutions in Tamil Nadu and since 2016 she is a professor from GRIET. She has authored over 26 research publications in international and national journals. Her areas of interest are Asynchronization Digital Circuits, Hardware Trojan Security in VLSI Design. She is a life member of IETE, ISTE and member of IEEE. She received project fund from various organizations like TNSCST and AICTE.

Dr.N.ArunVignesh received B.E.,degree in the Branch of Electronics and Communication Engineering from Anna University, Chennai in 2009, M.E., degree in Applied Electronics from Anna University, Coimbatore in 2011. He received his Ph.D. degree from Anna University, Chennai in 2016. Presently, he is working as an Associate Professor in the Department of Electronics and Communication Engineering, in Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad. His Ph.D. dissertation is focused on "Wireless Communications and Networking".

K. Jamal is presently working as a Associated Professor from ECE Department at GRIET, Hyderabad, India. He obtained B.Tech Degree in Department of ECE from JNTU, Andhra Pradesh, India and M.Tech in VLSI Design from Bharath University, Tamil Nadu, India. He is pursuing Ph.D from GITAM University, Andhra Pradesh, India. He has about 14 years of experience in teaching. His areas of interest include VLSI and Embedded Systems.