International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Analysis of Hardware Security to Prevent the Scan Based Attacks by using Sticky Counter

Rangu Lavanya
PG Scholar, Dept. of ECE,
CMRIT, Kandlakoy (v),
Hyderabad, Telangana, India

Dr. G. Shanmugapriya
Associate Professor, Dept. of ECE,
CMRIT, Kandlakoy (v),
Hyderabad, Telangana, India

Mr. S. Gopala Krishna
Assistant Professor, Dept. of ECE,
CMRIT, Kandlakoy (v),
Hyderabad, Telangana, India

ABSTRACT

Security of integrated circuits (ICs) has emerged as a major concern at different stages of IC life-cycle, spanning design, test, fabrication and deployment. Modern ICs are becoming increasingly vulnerable to various forms of security threats, such as: 1) illegaluse of hardware intellectual property (IP) \IP Piracy. 2) Illegal manufacturing of IC\ IC Piracy. Designing of confidential ICs must satisfy many design rules in order to rectify the various attacks and to protect the secret data. Based on the concept of withholding information, on-chip comparisons for actual and expected response. Obfuscation method to prevent the piracy overbuilding and reverse engineering RE. But no security against scan based attackers. This practical logic obfuscation applicable for combinational circuits and will not protect the scan attacks. In order overcome this drawback the recent works on hardware security to prevent piracy. From the security point of view, few limitations of existing method limit the security level. Some countermeasures have been proposed in order to secure the scan technique and on-chip comparison. This method can be applicable for both sequential, combinational circuits. This proposed method can be applied for all scan testing.

We implement the project using Xilinx ISE tool for Simulation and synthesis and the code is written in Verilog HDL.

Keywords: *Hardware security logic obfuscation, Flipped Scan Chain, On-Chip Scan Chain Comparison, AES*

I. INTRODUCTION

Traditionally, the IC design is written without any concern of obfuscation, and hence IC design is vulnerable to RE, piracy, and overbuilding. The gate-level netlist design to produce an obfuscated netlist, which is functionally equivalent to the former when correct key is given. An obfuscated gate-level netlist is synthesized into the layout geometry for manufacturing. An adversary buys the obfuscated IC on the open market and then obtains the gate-level netlist by image processing-based RE. However, the functionality of obfuscated cells cannot be identified. The modified netlist reacts with a silicon physical unclonable function (PUF), and it can exactly perform the same as that of the design as long as the correct license is issued by the IP/IC designer. This means that only the chips authorized by the designer can guarantee the correct functionalities. Obfuscation framework can prevent IC from RE, piracy, and over building. But no security against scan based attackers. This practical logic obfuscation applicable for combinational circuits and will not protect the scan attacks.

In order overcome this drawback the recent works on hardware security to prevent piracy to rectify the various attacks and to protect the secret data. From the security point of view, few limitations of existing method limit the security level. Some countermeasures have been proposed in order to secure the scan technique and on-chip comparison.

II. OBFUSCATION TECHNIQUE

Obfuscation technique is IC protection techniques inserting additional key gates (XOR or XNOR). One of the inputs to a key gate is the functional input in the design and the other is 1- bit key input. The correct key will be stored in a tamper- evident memory inside the design to prevent access to attackers. The logic obfuscation can protect the IC from piracy and overbuilding.

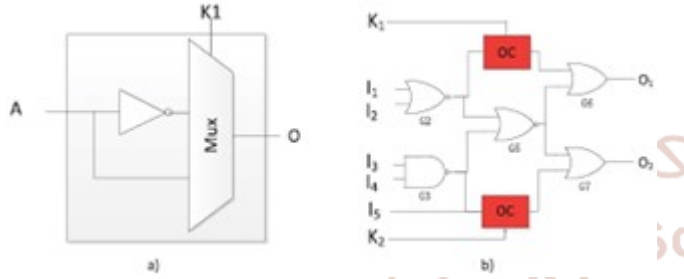

Figure: 1. Combinational logic obfuscation.
(a)Structure of an OC.
(b)An example of obfuscating a gate-level netlist with two OCs. An OC is used to replace an inverter or inserted into any wires in gate-level netlist.

In this obfuscation technique only the chips authorized by the designer can guarantee the correct functionalities. Hence, the obfuscation framework can prevent IC from RE, piracy, and overbuilding. The obfuscation cell (OC) is composed of an inverter and a Multiplexer.

The structure is shown in Figure: 1(a), where the key is a select input of the multiplexer (because of the key's importance, a distribution framework must be established so that the IP designer can securely unlock each IC). To replace an inverter with the OC or insert the OC into any wire of gate-level netlist. In Figure: 1(b), a simple circuit is obfuscated by two OCs.

PUF-based obfuscation and the generation of the license:

The PUF response interacts with obfuscation cell to generate a chip-dependent license to prevent piracy attacks. An attacker with no information about the key of the OCs cannot compute the correct license to unlock the pirated chips.

The designer is the only one who can issue the license to activate the chip. The generated configuration is stored in the flip-flops to unlock the chip. PUF response is used to unlock the function of the chip without the correct PUF response, the function would not perform correctly. There-fore, the circuit is kept locked until the correct license unlocks it. An example for generating the license in Figure: 2. Considering four OCs in Figure: 2, OC1–OC4 and *K*1–*K*4 are the key bits of the OCs. Assume *K*1–*K*4=1010, the OC can be used to replace value is 0110. To possibly active the chip, the 4-bit PUF output 0110 should be XOR'd with a 4-bit license that is able to generate the result of 1010. (In this case, the license should be 1100). The chip can be correctly unlocked with the calculated license and the PUF response.

This obfuscation technique applicable for combinational circuits will not protect the scan based attacks.

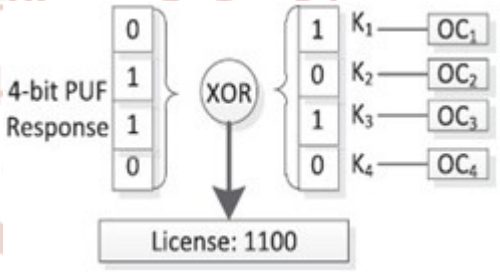

Figure: 2.PUF-based obfuscation and the generation of the license.

In order to overcome this draw back the recent works on hardware security with sticky counter to prevent the scan based attacks in the proposed method

III. PROPOSED SCHEME

Block diagram:

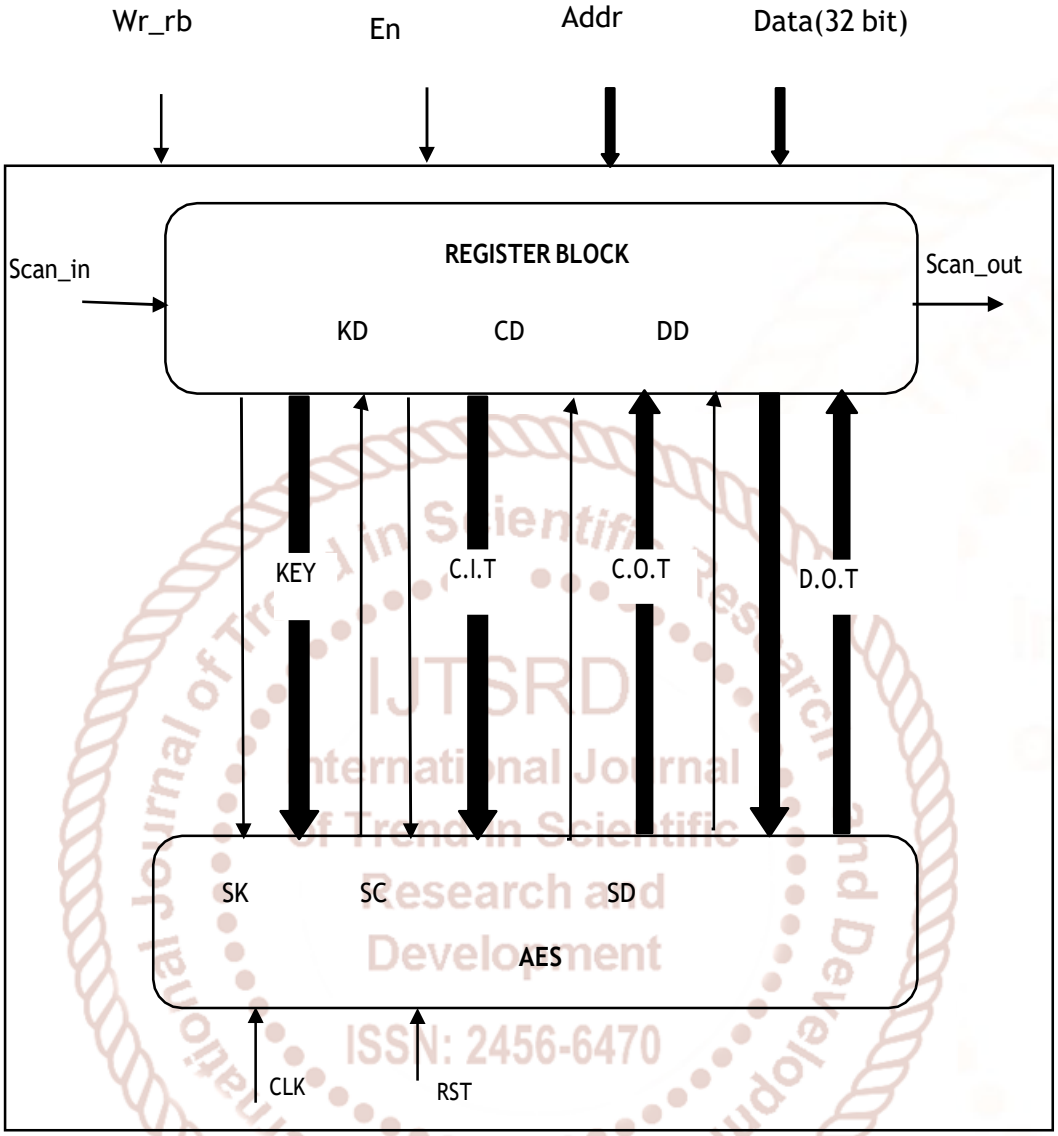

Figure: 3 Block diagram

Wr_rb	write read bar
En	Enable
Addr	Address
Data	32 bit Data
KD	Key Done
CD	Cipher Done
DD	Decrypt Done
SK	Start Key
SC	Start Cipher
SD	Start Decrypt
KEY	128 bit of Key
C.I.T	128 bit Cipher Input Text
C.O.T	128 bit Cipher Output Text
D.I.T	128 bit Decrypt Input Text
D.O.T	128 bit Decrypt Output Text

REGISTER BLOCK						
0	Key [31:0]					
1	Key [63:32]					
2	Key [95:64]					
3	Key [127:96]					
4	Cipher Input text [31:0]					
5	Cipher Input text [63:32]					
6	Cipher Input text [95:64]					
7	Cipher Input text [127:96]					
8	Cipher output text [31:0]					
9	Cipher output text [63:32]					
10	Cipher output text [95:64]					
11	Cipher output text [127:96]					
12	Decrypt Input text [31:0]					
13	Decrypt Input text [63:32]					
14	Decrypt Input text [95:64]					
15	Decrypt Input text [127:96]					
16	Decrypt output text [31:0]					
17	Decrypt output text [63:32]					
18	Decrypt output text [95:64]					
19	Decrypt output text [127:96]					
20	startDecrypt	startCihper	Startkey	DecryptDone	ChiperDone	keyDone

Figure: 4 Register block

Basic scan chain:

Scan chain is a technique used in design for testing. The objective is to make testing easier by providing a simple way to set and observe every flip-flop in an IC. The basic structure of scan include the following set of signals in order to control and observe the scan mechanism.

- Scan_in and scan_out define the input and output of a scan chain. In a full scan mode usually each input drives only one chain and scan out observe one as well.
- A scan enable pin is a special signal that is added to a design. When this signal is asserted, every flip-flop in the design is connected into a long shift register.

Figure: 5. Scan chain.

Clock signal which is used for controlling all the FFs in the chain during shift phase and the capture phase. An arbitrary pattern can be entered into the chain of flip-flops, and the state of every flip-flop can be read out.

Advanced Encryption Standard (AES):

Advanced Encryption Standard, also known by its original name Rijndael (Dutch U pronunciation), is a specification for the encryption of electronic data established by the S. National Institute of standards and technology (NIST) in 2001.AES is a subset of the Rijndael cipher developed by two Belgian crypto graphers, vincent Rijndael and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES became effective as a federal government standard on May 26, 2002, after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved by cryptographic module.

Registers in register block connected in scan chain

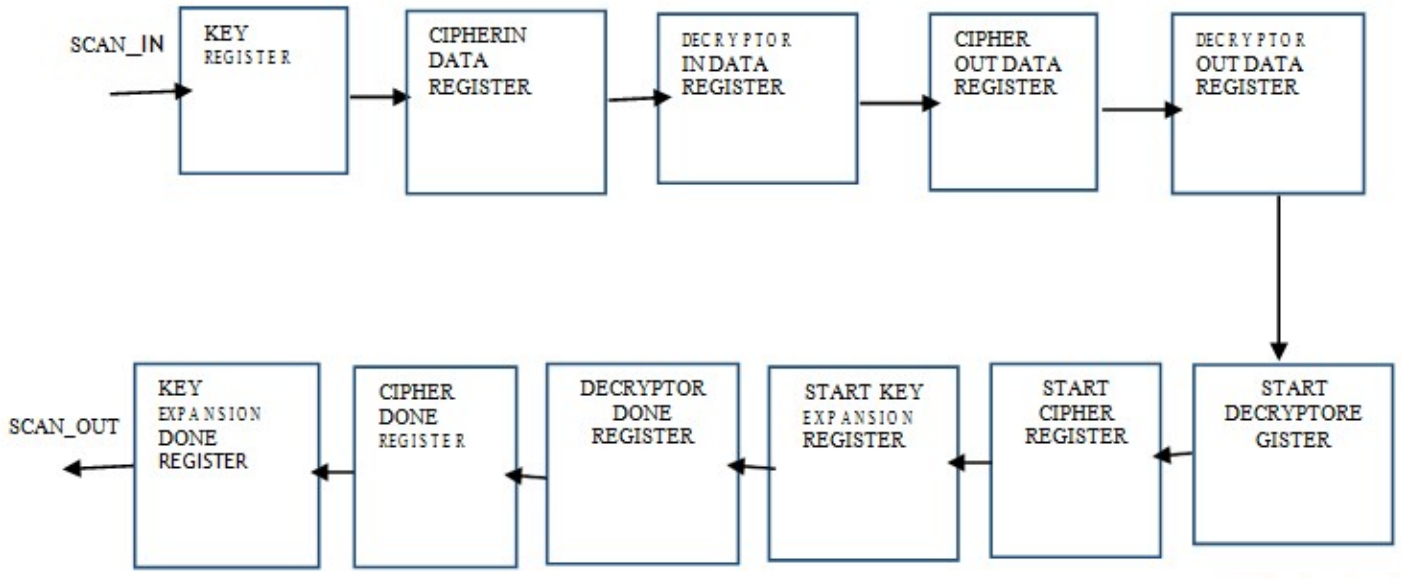

Figure: 6 Registers in register block connected in scan chain

The register block of our design contains 20 registers of 32 bits each. The registers are reserved for key, cipher input data, cipher output data, decryptor input data, decryptor output data and the status and control bits –start key expansion, start encryption, start decryption, key expansion done, encryption done and decryption done. All of these registers are connected serially in a scan chain as indicated below. The registers key, cipher input data, cipher output data, decryptor input data, decryptor output data are 128

bits each while the registers start key expansion, start encryption, start decryption, key expansion done, encryption done and decryption done are 1 bit wide. In scan mode, when scan_en is applied the data is shifted serially from scan_in to "key" to "cipher_in_data" to "decryptor_in_data"to"cipher_out_data"to"decryptor_out_data"to"start_decryptor"to"start_cipher"to"start_key_expansion"to"decryptor_done"to"cipher_done"to "key_expansion_done" to scan_out. We have inserted inverters on the scan chain to implement the flipped scan chain model. The register blocks scan chain as show in figure: 6

Combinational circuits with scan flip flop:

This approach based on comparing the actual responses with the expected responses within the chip area instead of scanning-out and comparing the response within the ATE. In standard scan-based scheme, FF's is replaced with scan flip flops (i.e. flip flop with a multiplexer). These are connected serially to behave as long shift register in test mode. The input of FF is directly connected to input pin (scan-in) and the output of the FF is directly connected to scan-out (output pin). An additional pin (scan enable) is accessed to select whether the SFFs behave as normally or as a shift register. The output of one SFF is connected to the input of next SFF.

When the scan chain is introduced for hardware testing, additional scan enable pin is needed to enable the test mode from normal mode. Insertion of scan-chains while testing the hardware requires a few multiplexed pins to the standard inputs/outputs to behave as the scan-enable, scan-inputs and scan-outputs. A scan DUT with additional mux is shown in the Figure: 7

The circuit of a sequential logic which comprises of combinational circuits and flip flops. It can be observed that there is a mux in front of each flip flop which is called scan mux.

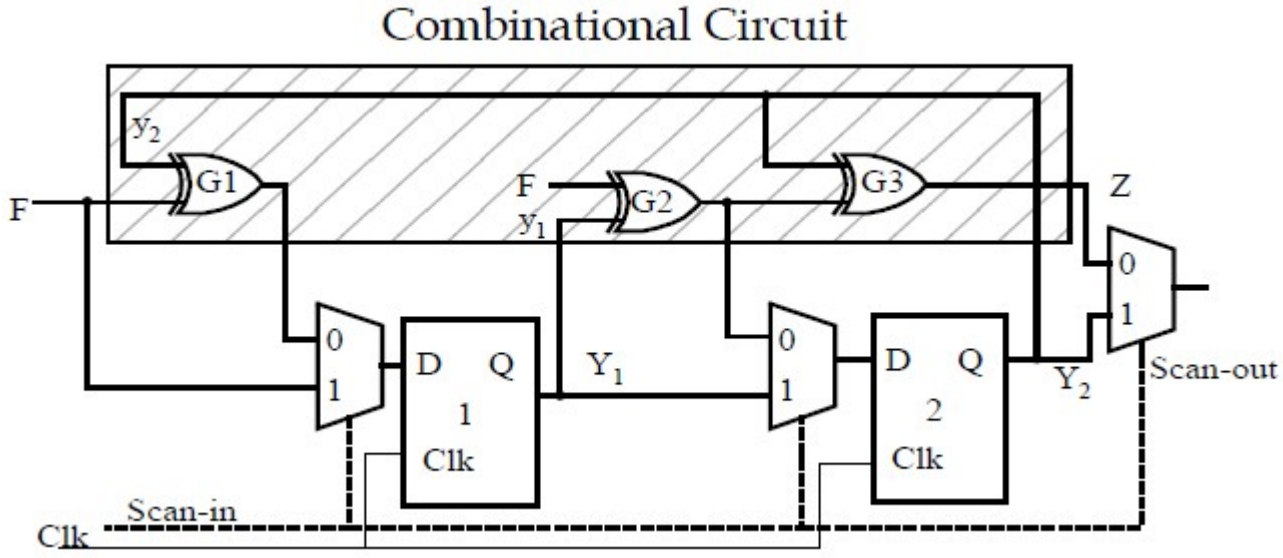

Figure: 7 Combinational circuit with scan flip flop.

The flip flop and the mux together are called scan enable Flip Flop. The select line of these muxes are scan mux. The flip flop and the mux together are called scan enable Flip Flop. The select line of these muxes are tied to a global signal called scan_enable. When scan enable is "1", the flips flops are arranged serially as a shift register bypassing all the combinational logic.

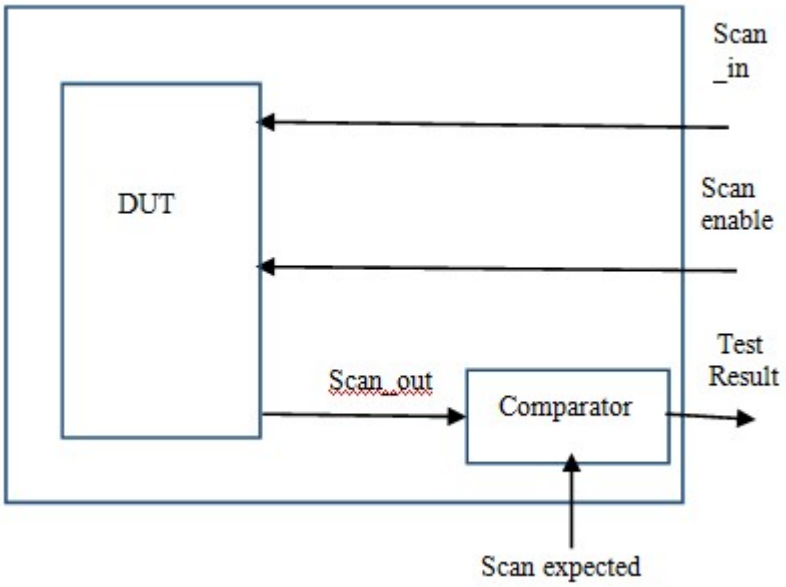

Figure: 8 Test circuit without sticky counter.

As shown in figure: 8, when "scan_en" is applied the "scan_input" shifts serially through the registers and appears at the "scan_out" pin of the circuit after several cycles. The number of cycles depends on the length of the scan chain i.e the number of flip flops connected seriallyt in the scan chain. To test the correctness of the output, we supply the expected values at the "Scan_exp" pin and the result of the comparison which is done by the comparator inside the chip appears at the "test_result" output pin.

This setup suffers from a serious security flaw. As we know that software is responsible for generating the key based on the result of negotiations with the communication partner and other dependencies. The software is responsible (FSFFs). An additional inverter is added along with the scan chain (i.e. securable, SFFs is replaced with flipped scan chain flip flops Flipped scan chain).When the inverter is randomly arranged before the scan chain, the scan out data of random SFF will be flipped (inverted). Flipped Scan chain aimed at protecting the scan data form being analysed through the intermediate states of the device. Moreover, this FSFF does not impact on the normal functionality of the device.

An introduction of inverter in the scan chain to get a flipped scan chain as shown in figure.3.4. Flipped scan chain. This will guarantee that the register bits do not appear as is at the scan out as the position of the inverters are random and known only to the designer/ design house. However, the position of the inverters can be realized by carefully applying select values at scan_in and observing scan_out, though very tedious. Flipped scan chain increase the complexity of brute force attack to observe the intermediate signals exactly. Further, random arrangement of NOT gate inverts the test output randomly and goes for comparison with the same flipped expected response. Based on the approach of On-chip comparison, this paper in brief is to compare the actual response with the expected response for whole test vector and even no more unknown values in the test data make it easy to provide expected response after testing the data with flipped scan chain. When the scan chain is enabling, need to provide both expected and test input to the design. But predicting the expected response for unknown values in the test input is no longer possible.

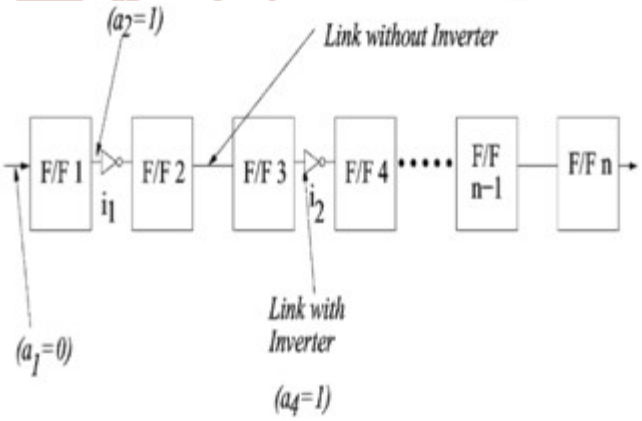

Figure: 10. Security analysis of the flipped scan chain

Circuit to add a sticky comparator:

The second change is to modify the test circuit to add a sticky comparator and a bi-directional output buffer. In such case, this comparison will no more confidential and effective.To overcome this limitation, the proposed approach is to compress the input test data by code based scheme. Data compaction method will reduce the unknown values by making it compatible within the test patterns. The general scheme of the proposed Secure Comparator is shown in Figure 11. Instead of neither ignoring the comparison result for unknown values nor providing the additional mask to avoid the unknown values in the comparison, these unknown values are filled by using the compression technique from the flipped scan chain. Once the data is compressed with known values, ATE also provides expected response for those compressed test inputs. Instead of scanning out the data, on- chip comparison is done by secure comparator. The Secure Comparator is composed of three parts: the Sticky Comparator, output enabler and I/O buffer. Sticky comparator compares the scan out result with the expected response the help of a flag. Initially the flag is reset, the flag set to '1' when the comparison fails. The value of the flag designates whether it is equal or not. The output enabler triggers the test Res after applying the whole test vector. It consists of down counter with parallel load to load the #SFF when the scan chain is enabling. I/O buffer (bidirectional buffer) permit the sharing of same pin for both Test Res and Sin.

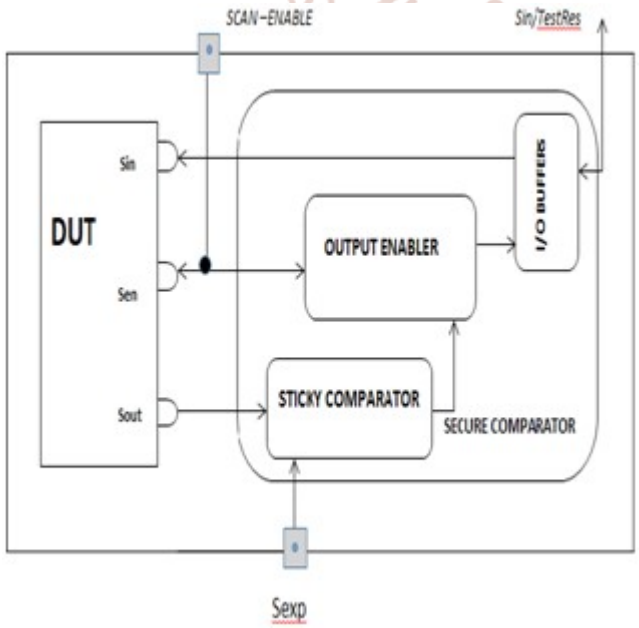

Figure: 11 Secure comparator

Test bench of scan chain:

The sticky comparator accumulates the test result over the entire test sequence until externally reseted, i.e. in a period of 100 cycles, if the comparison failure happens at the 20th bit, sticky comparator hold the test_result as fail throughout the rest of the test irrespective of subsequent bits resulting in a comparison pass or fail. By reading the test result after a lot of cycles will not allow to determine the comparison fail cycles and thereby the exact scan_out bits cannot be determined. However, by reading out the test_result for every cycle can guarantee the determination of the scan_out bit exactly like the previous circuit. We can prevent this by adding an I/O buffer which muxes the two pins "scan_input" and "test_result" onto the same pin. Since both the above signals have opposite direction i.e. scan_input is input to the IC and test_result is the output of the chip, both cannot be active at the same time. The direction of the I/O buffer is controlled by the "scan_enable" pin. If scan_enable is high, the I/O buffer behaves like an input pin and the value of the pin is propagated to the scan_input of the circuit. If scan_enable is low, then the I/O buffer behaves like and output pin and the value of the comparator output (test_result) is propagated to the I/O pin and scan_input is cut off from the pin. To observe the output of the sticky comparator at the output pin, scan_enable has to be set to "0", which in turn disables the scan path and the values of the combinational logic are pushed onto the flip flops and the values inside the scan chain are destroyed and no longer relevant. Since the combinational logic functionality is unknown to any unauthorized parties, it is simply impossible to scan in known values and guess the location of inverters on the scan chain by observing the scan_out as the scan chain data is corrupted when scan_enable is set to "0" and thus, the circuit in figure: 7 combinational scan flip flop, is suitable to both testing by supporting scan chain and providing security.

IV. SIMULATION AND SYNTHESIS RESULTS

Scan chain:

A scan enable pin is a special signal that is added to a design. When this signal is asserted, every flip-flop in the design is connected into a long shift register. Scan chain can be in combinational circuit and it can be used for testing purpose.

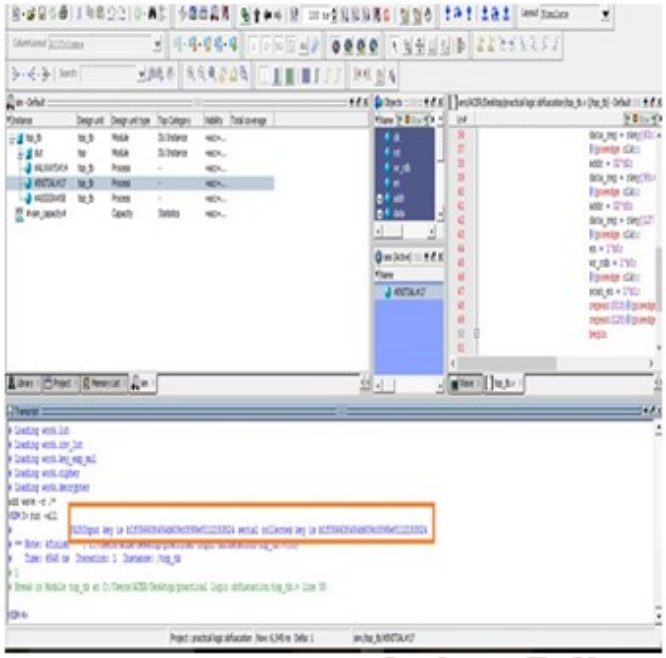

Figure: 12 Scan chain run out

In this scan chain whatever the key bits are given to the scan chain is same as the output of the scan chain. The input key b1f056638484d609c0895e8112153524 then the resulted outputof serial collected data is b1f056638484d609c0895e8112153524. Therefore the input key is same as the serial output data. There is no security to the data.

Scan chain simulated wave form:

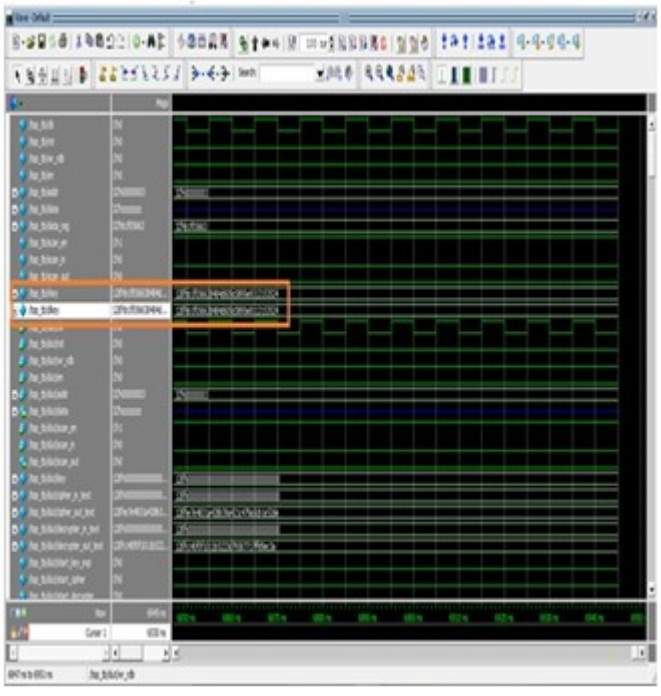

Figure:13 Simulated wave form.

resulted data. The above security flaws can be overcome by 2 modifications as shown in below

Flipped scan chain:

In the circuit to insert inverters randomly in the scan chain to get a flipped scan chain. This will guarantee that the register bits do not appear as is at the scan out as the position of the inverters are random and known only to the designer/ design house. However, the position of the inverters can be realized by carefully applying select values at scan_in and observing scan_out, though very tedious.

Test bench of flipped scan chain:

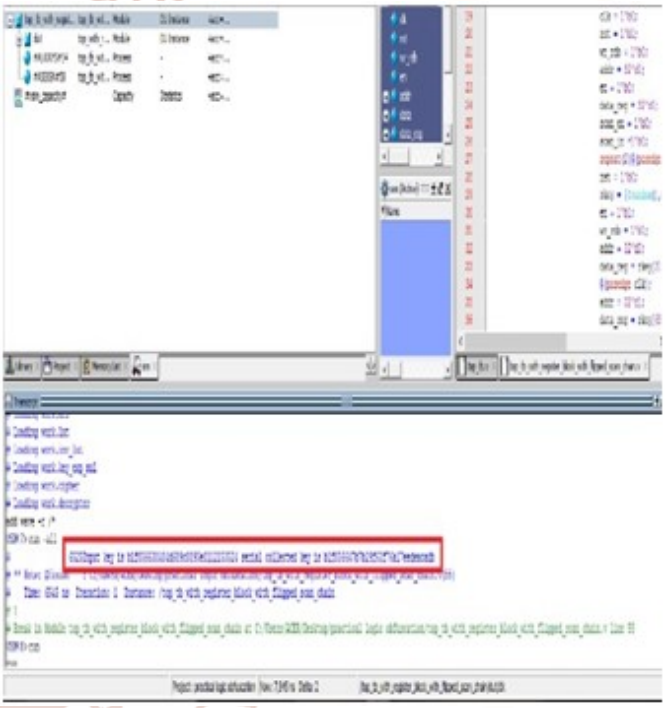

Figure: 14 Flipped scan chain run output.

In this additional inverter is added along with the scan chain the key can flipped. The given input key as b1f056638484d609c0895e8112153524 the serial collected key is b1f056647b7b29f63f76a17eedeacadd these can be shown in figure:14 the selected portion is the resulted output.

Flipped scan chain simulated wave form:

When the inverter is randomly arranged before the scan chain, the scan out data of random SFF will be flipped. Flipped scan chain protecting the scan data. This FSFF does not impact on the normal functionality of the device. These simulated

waveform can be show the input key to the serial output key. Selected particular portion is the simulation result. When the inverter is randomly arranged before the scan chain, the scan out data of random SFF will be flipped.

Flipped scan chain protecting the scan data. This FSFF does not impact on the normal functionality of the device. These simulated waveform can be show the input key to the serial output key. Selected particular portion is the simulation result

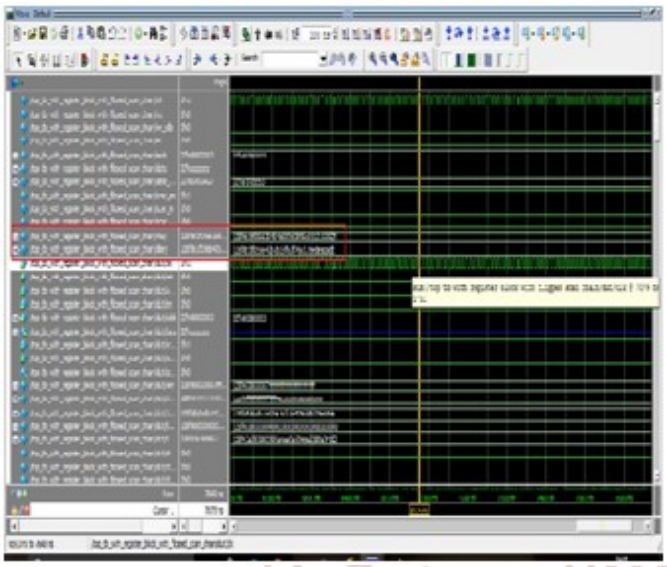

Figure:15 Flipped scan chain wave form

Sticky comparator

This is the second change is to modify the test circuit to add a sticky comparator and a bi-directional output buffer. Sticky comparator hold the test_result as fail throughout the rest of the test irrespective of subsequent bits resulting in a comparison pass or fail.. If scan_enable is high, the I/O buffer behaves like an input pin and the value of the pin is propagated to the scan_input of the circuit. If scan_enable is low, then the I/O buffer behaves like a output pin and the value of the comparator output (test_result) is propagated to the I/O pin and scan_input is cut off from the pin.

Test bench with sticky comparator:

Sticky comparator compares the scan out result with the expected response the help of a flag.in this sticky comparator input key is 06b97b0db1f056638484db609c0895e81.Then the resulted output 06b97b0a4e0fa99c7b7b29f63f76a17e is as shown in figure:16.

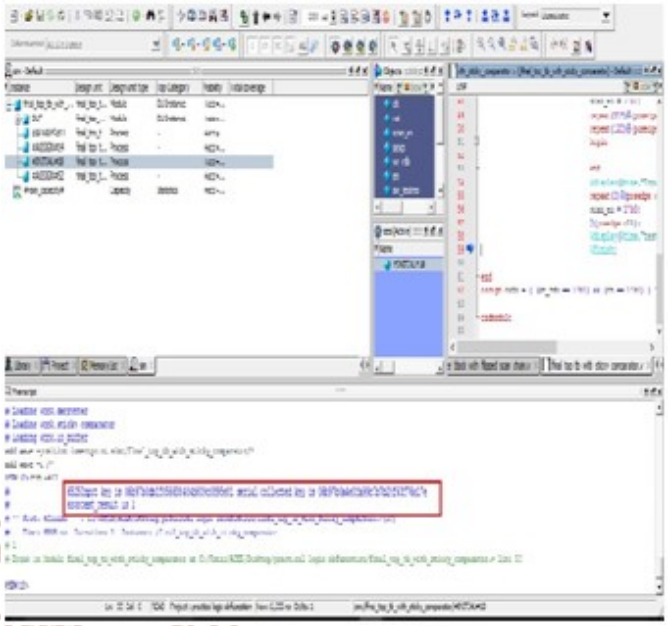

Figure: 16 Sticky comparator run output

Sticky comparator wave form:

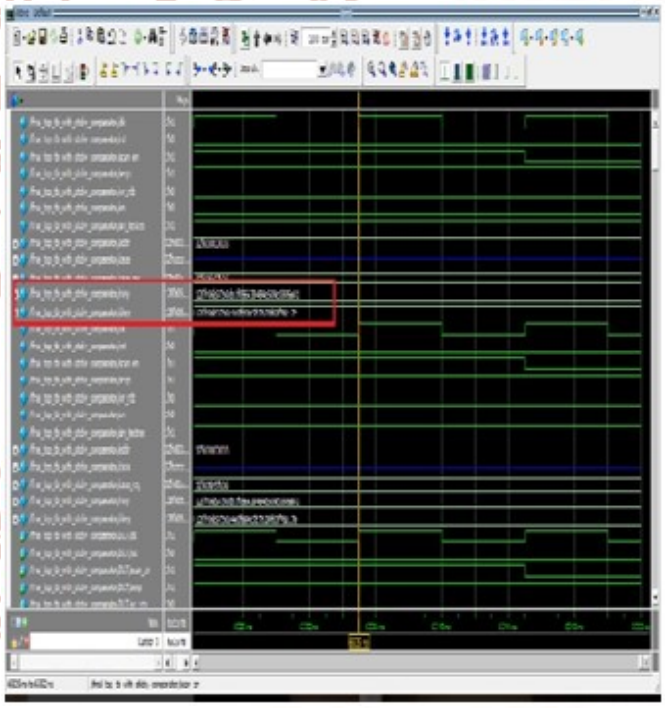

Figure: 17 Sticky comparator simulated wave form

The sticky comparator accumulates the test result over the entire test sequence until externally re-setted.

Test result wave form:

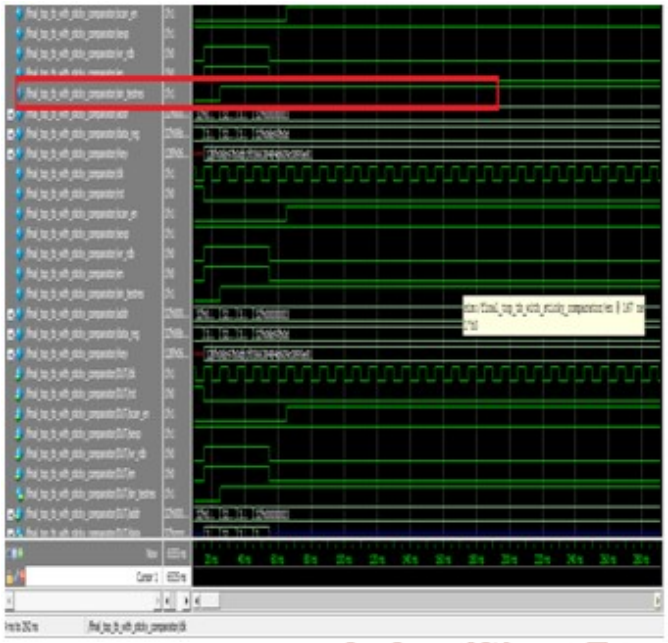

Figure:18 Test result wave form.

In this test result we can apply a constant "0/1" to the Scan_exp pin and based on the result of the comparison (test_result) we can find out the value of the scan_out. For example, if scan_exp is tied to "logic 0", then a value of "1" at scan_out will generate a "Fail" at the test_result and a value of "0" at scan_out will generate a "Pass" at the test_result pin. Based on Pass/Fail at the test_result pin.

CONCLUSIONS

In this proposed scheme, a new approach of flipped on-chip comparison is described for security issues. Based on the concept of holding the confidential information within the chip, proposed method is more secure than other countermeasures with less controllability to unknown users. It compares both the input response and the expected response without relying on the cost of the design. Flipped scan chain increases with negligible area overhead and design changes. This method has also been accessed in order to reduce the possible unknown values in the test procedure. On comparing with the standard scan test, this design does not impact on the quality of the test and the diagnosis of fault.

Applications:

- This method can be applicable for both sequential and combinational circuits
- Hardware security protect the secret data and preventing the piracy overbuilding and reverse engineering RE
- This hardware security of combinational flip flop is suitable to both testing by supporting scan chain and providing security.

Future scope:

In a large circuit, there are lakhs of flip flops. If all the flip flops are stitched in a single chain, the delay of the scan chain is huge and is a problem to the testing process and time taken to test is very high and it becomes costly. We can split the flop into multiple scan chains. The flip flops of the key register can be put under several parallel scan. chains. This can be enhance the security further to our implementation architecture.

REFERENCES

1. Lavanya R. "Hardware security with sticky counter to prevent the scan chain based attacks".International journal of VLSI system.Design and communication system ISSN 2322- 0929 Vol.05, Issue.06, june-2017,pages:0588-0591.
2. Jiliang Zhang,"A practical logic obfuscation for hardware security," IEEE transactions on very large scale integration (VLSI) system. Vol.24.no.3.march 2016.
3. Poehl F, Beck M, Arnold R, Rzeha J, Rabenalt T, Goessel
4. M. On-chip evaluation, compensation and storage of scan diagnosis data. IET Computers & Digital Techniques. 2007: 1(3):207–12.
5. Yang B, Wu K, Karri R. Secure scan: a design-for-test architecture for crypto chips. IEEE Transactions on Computer- Aided Design of Integrated Circuits and Systems. 2006 Oct; 25(10):2287–93.
6. Yang B, Wu K, Karri R. Scan based side channel attack on dedicated hardware implementations of data encryption standard. Proceedings of IEEE International Test Conference. 2004 Oct. p. 339–44.
7. Sengar G, Mukhopadhyay D, Chowdhury DR. Secured flipped scan-chain model for crypto-architecture. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2007 Nov; 26(11):2080–4.

8. Hely D, Bancel F, Berard N, Flottes ML, Rouzeyre B. Test control for secure scan designs. Proceedings of the IEEE European Test Symposium; 2005 May. p. 190–5.
9. Chiu G–M, Li JCM. A secure test wrapper design against internal and boundary scan attacks for embedded cores. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2012 Jan; 20(1):126–34.
10. Agrawal M, Karmakar S, Saha D, Mukhopadhyay D. Scan based side channel attacks on stream ciphers and their
11. counter-measures. Proceedings of 9th International Conference on Cryptology in India; Kharagpur: LNCS; 2008. p. 226–38.
12. Da Rolt J, Di Natale G, Flottes ML, Rouzeyre B. Thwarting scan-based attacks on secure-ICs with on-chip comparison. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2014 Apr; 22(4):947–51.
13. Da Rolt J, Di Natale G, Flottes ML, Rouzeyre B. New security threats against chips containing scan chain
14. structures. IEEE International Symposium; Hardware- Oriented Security Trust; 2011 Jun. p. 110–5.
15. Hely D, Bancel F, Flottes M, Rouzeyre B, Renovell M, Berard N. Scan design and secure chip. Proceedings of the IEEE International On-Line Testing Symposium; Funchal, Portugal: 2004. p. 219–26.
16. Easter RJ, Chencinski EW, D'Avignon EJ, Greenspan SR, Merz WA, Norberg CD. S/390 parallel enterprise server CMOS cryptographic coprocessor. IBM Journal of Research and Development. 1999 Sep-Nov; 43(5/6):761– 76.
17. Josephson D, Poehhnan S. Debug methodology for the McKinley processor. Proceedings of International Test Conference; Baltimore, MD: 2001. p. 451–60.
18. Mukhopadhyay D, Banerjee S, Chowdhury DR, Bhattacharya B. Cryptoscan: Secured scan chain architecture. Proceedings of 14th IEEE Asian Test Symposium; 2005. p. 348–53.
19. Lee J, Tehranipoor M, Patel C, Plusquellic J. Securing scan design using lock and key technique. Proceedings of the 20th IEEE International Symposium of Defect and Fault Tolerance in VLSI Systems; 2005. p. 51–62.
20. Shi Y, Togawa N, Yanagisawa M, Ohtsuki T. Robust secure scan design against scan-based differential cryptanalysis. IEEE Transaction onVery Large Scale Integration (VLSI) Systems. 2012; 20(1):176–81.
21. Sridhar KP, Saravanan S, Sai RV. Countermeasure against side channel power attacks in cryptography devices. Indian Journal of Science and Technology. 2014 Apr; 7(S4):15–20.
22. Sridhar KP, Raguram M, Prakash B, Koushighan S, Saravanan S. Secured elliptic curve cryptosystems for scan based VLSI architecture. ICICE2014-IEEE explorer; Chennai: 2014. p. 1–5.
23. Saravanan S, Charaphani K, Silambamuthan R. Design and implementation of hardware based entropy analysis. Research Journal of Applied Sciences, Engineering and Technology. 2012; 4(14):2082–6.
24. Narmatha D, Saravanan S. Improved observability of test pattern using X-alignment technique. International Journal of Applied Engineering Research. 2014; 9(11):1711–9.

Authors Profile:

Rangu Lavanya received her bachelor's degree in 2015 in electronics and communication engineering from Trinity College of engineering and technology peddapalli, India which is affiliated with JNTU Hyderabad, India. Her areas of interest include VLSI design. she is pursuing her M-Tech in VLSI system design from CMR Institute of technology.

Dr. G. Shanmugapriya has completed Ph.D. from OPJS University, Rajasthan and Master of Engineering with specialization in CCE (Computer and Communication Engineering) from Anna University (Chennai, Tamilnadu) and Bachelors of Engineering with specialization in ECE (Electronics and Communication Engineering) from Bharathidasan University at Tiruchirapalli, Tamilnadu). She started her career as an Assistant Professor in School of Computing at Sastra University (Thanjavur, Tamilnadu). During this period she was involved also in designing of new projects besides project guidance and teaching. As a part of her software development program she moved to Germany and worked as a project engineer. She is also a Microsoft certified person and underwent a

couple of Microsoft Approved courses such as Advanced Foundations of Microsoft .NET 2.0 Development and Advanced Data Access with Microsoft Visual Studio to add more skills to software development. She worked as an Associate Professor at St. Peters Engineering College at Hyderabad prior joining at CMR Institute of Technology as an Associate Professor. During this period she guided various projects in both M. Tech and B. Tech level students in the field of communication Engineering. Her major areas of interest are Electromagnetic theory, Antennas and wave propagation and Microwave Engineering. With her vision she intends to provide quality education to students with application oriented knowledge in association with CMRIT.

Mr.S. Gopala Krishna is working as an assistant professor in CMR Institute of Technology. He had 3 years of experience in teaching field. He had completed of B. Tech (ECE) from Drupal Raj Engineering College. This is affiliated to Jawaharlal Nehru Technological University Hyderabad. Andhra Pradesh, India. He had done Master's degree in Embedded Systems from Vivekananda institute of technology &science which is affiliated to Jawaharlal Nehru Technological University Hyderabad, Andhra Pradesh, India