On-Chip Comparison based Secure Output Response Compactor for Scan-based Attack Resistance

Sudeendra kumar K, Kalpesh Lodha, Sauvagya Ranjan Sahoo, K.K.Mahapatra
National Institute of Technology, Rourkela, India.

***Abstract*- Confidential Information transactions need cryptographic algorithms to give access to data only for authenticated individuals. In the era of smart phones and internet of things, most of the data exchange occurs between small and smart electronic gadgets. Cryptographic algorithms are necessary in smart gadgets to secure the sensitive data. Hardware implementations of cryptographic protocols on ASIC/FPGA devices are subject to various attacks from adversaries. In literature, we can find various attacks based on scan chain. The scan chains or Design for Testability (DFT) is included in the design to improve testability can become potential backdoors to conduct attacks. And also we can find several countermeasures to protect leaking of sensitive information in scan chains can be found in literature. One such technique is based on-chip comparison scheme. In this paper, we propose novel architecture for on-chip comparison circuit, which enhances the security and also reduces the test time of the circuit. The experimental result confirms the test time reduction.**

Keywords: **On-chip comparison, Security, Scan-based attack, Side-channel attack, ATE, design for testability (DFT), signature register.**

I. INTRODUCTION

Structural testing is mandatory for every IC manufactured, before shipping it to the customer. In fabrication of CMOS devices, small amount of chips manufactured may not work properly. To improve the quality of testing and to reduce the cost of testing, Design for Testability (DFT) is in use from last two decades. DFT includes insertion of scan chains to increase the observability and controllability of nodes inside the circuit. DFT insertion replaces the flip-flops in the design with scan flip-flops (SFF). The SFFs are connected to form shift register and scan chain. Generally scan chains will have input pin (scan in), output pin (scan out) and enable pin (scan en). When enable pin is low, the scan chain is inactive and design works in functional mode, and when enable is high, design works in test mode. [1]

The cryptographic algorithms are used in electronic data exchange to guarantee the security and authenticity of the data transactions. In recent times, many embedded system applications demand cryptographic algorithms and implementing these algorithms in dedicated hardware is required for performance optimization. The cryptographic techniques are also useful in hardware intrinsic security. During test mode, SFFs are connected to form scan chain and stream of bits pumped into the design can be shifted through scan chain to get the data out through the scan out pin. By Switching the chip from functional mode to test mode attacker can make use of scan structures to observe confidential data. [2]

The possible solution to solve this security threat is to blow the fuse, which will physically disconnect the scan chains after manufacturing test. Physically disconnecting the DFT will impede the testing the chip post production which is important for cryptographic chips to check the correct functional behavior of design. Scan disconnection hampers diagnosis of chip. Success of attack depends upon the expertise of attacker related to cipher algorithm, scan structure, laboratory setup for differential power analysis (DPA), access to design database. The availability of de-cap and microprobe station to trace internal signals will be a great advantage for attacker to perform successful attack [3][4].

The first scan based attack on DES (Data encryption standard) was proposed in [5]. In [5], Yang et al. describe the procedure to retrieve the DES first round key by finding the data in first intermediate register in scan chain. In [6], same authors propose differential scan attack on Advanced Encryption Standard (AES). The input messages causing hamming distance equal to 1 are XORed to obtain the part of the secret key. The complete secret key can be obtained by repeating the same procedure with different input messages. Attack on public key ciphers like RSA and ECC is described in [7] and [8] respectively. The attack is based on using the scan structures to read the intermediate registers and leak out the key through scan out.

The cost of testing can be reduced using advanced DFT structures like test compression schemes. Several test compression schemes are described in literature, but most significant techniques are standard industrial compression methods like Adaptive Scan supported by Synopsys, OPMISR by Cadence and EDT by Mentor Graphics [9]. In [9], security analysis of three industrial test compression schemes is described. Security analysis concludes all three schemes are vulnerable to attack. Success rate of attack varies from technique to technique and depends upon number of active scan chains in the design. In [10], a new DFT architecture has been proposed. This technique makes use of on-chip comparison technique to withhold the information leaking through the output pin. The on-chip comparison techniques will reduce the test data volume transferring from DUT to ATE. On-chip comparison is performed between actual response and expected response from the DUT. This test method is described in [11][12]. On-chip comparison technique is used to enhance the security against scan attacks in [10].

Several countermeasures are proposed by researchers to defend scan attacks, without affecting manufacturing test.

978-1-4799-7926-4/15/$31.00©2015 IEEE

Three categories are found in literature: dedicated secure test wrappers, scrambling and obfuscation of real content inside the scan chain and on-chip comparison technique. Section II summarizes the countermeasures against scan attacks and discusses their drawbacks. In this paper, we primarily focus on using on-chip comparison technique to enhance the defence against scan attacks. The security analysis and testability analysis is performed on proposed technique. Area utilization and test time calculations are presented.

Rest of the paper is organized as follows: Section II discusses relevant DFT techniques and their security aspects. The proposed on-chip comparison technique design and implementation is given in section III. Section IV describes implementation, and section V discusses security and testability of proposed technique. Finally, Section VI concludes the paper.

II. PRELIMINARIES

An important solution found in literature against scan attacks is based on secure test wrappers. These wrappers are deployed around the DUT interface to control the test access mechanism. The commonly used test interface is JTAG standard. The JTAG FSM works in functional mode and test mode. The JTAG FSM is modified and secure test wrappers are inserted. Most of the secure test wrapper implementations are based on locking/unlocking mechanism to execute JTAG instructions. Few solutions also target IEEE 1500 test wrapper and similar locking/unlocking mechanism is described. Generally secret keys will be provided to authenticated users to lock and unlock the test port access [13][14]. But key management is an open issue in these techniques. For a limited number of chips produced, these techniques are quite successful. In the large scale production of chips, it is impossible to store keys and challenge response pairs (CRP's). In [15], authors propose physical unclonable function (PUF) based challenge response pairs to lock and unlock the test access. Commercial solutions like [16] ARM Trustzone gives an option to blow up JTAG interfaces and test access is permanently blocked. Secure test wrappers requires implementation of some or the other crypto function, which gets add to the area and timing overhead.

Scrambling and obfuscation is another type of defence against scan attacks. When the key inserted is not valid, countermeasure will scramble data at the scan output to confuse the attacker or will restrict the further access. Scrambling is proposed in [17] [18]. Da Rolte in [19] proposes a test solution which forbids the secret information flowing out. Separate monitors or sensors are designed to check the confidential information scan chains. Pumping out sensitive data is not allowed. Security through obfuscation of scan chains is proposed and it is shown ineffective against Differential Scan Attack (DSA) in [20]. The authors of [21] propose the addition of inverters in between the scan flip-flops. This will confuse the attacker doing timing based attacks, but ineffective against differential power analysis. In [22], the authors propose addition of XOR gates between the scan chain flip-flops, and this technique is also vulnerable to DSA.

A sophisticated attacker having access to microprobing equipment and expertise to use it can easily trace the signals inside the chip and all the countermeasures discussed above are vulnerable. In [23], authors propose adding a spy flip-flop in between the scan chain, which is always loaded with constant in normal operation and when scan enable is disabled and illegal shifts occur in scan chain, spy flip-flop will pump the constant into scan chain. Still this technique is vulnerable to de-cap based tracing attack. Microprobing station is costly and expertise in using it is also a rare. So probing based attacks is not so easy.

Built in Self Test (BIST) techniques are very helpful as a countermeasure against scan attacks. Cryptographic cores can act like input pattern generators and output response schemes used in BIST techniques will only produce PASS/FAIL signatures at scan out [24]. So BIST techniques are promising solution against scan attacks, if diagnostic resolution is not a requirement. Block ciphers can be used as both pattern generator and response compaction as suggested in [25]. The threats and attacks described in [20] clearly shows that techniques used in [6, 9, 16] are vulnerable.

Another countermeasure found in literature is based on response compactors. In [26], authors describe the countermeasure based on output compaction and X-masking. The compactor scrambles the test data in so complex way that it is impossible to retrieve the data in scan chain. Even this technique is also vulnerable to the attacks described in [20].

Authors of [10] propose the technique based on on-chip comparison technique to countermeasure the scan attack. This is another form of output compaction scheme, used in BIST techniques with low diagnostic capabilities. Authors describe the advanced DFT architecture, in which diagnostic capability is not compromised.

The output coming from the scan out is compared on-chip to produce the PASS/FAIL signature in [10]. ATE will feed in the expected response into the on-chip comparator to generate the signature. ATE Test engineer will have access to confidential information coming out of the scan out. This is one drawback in this technique. Another way to retrieve the sensitive information is by applying brute-force attack. Brute force attack requires $2^{\#SFF}$ attempts. It is easy to perform successful brute force attack when number of flip-flops is small in number in scan chain.

In this paper, we extend the work presented in [10], to avoid the sharing of sensitive data for ATE programming and also analyze the area and test time.

III. MAIN IDEA

LFSR is similar to a shift register configuration, but has mod_2 addition feedback from selected stages along register to form serial input to the first stage [12]. A primitive

polynomial, defining the feedback for LFSR of length N, is chosen that will progress in pseudo-random manner through 2^N-*1* states before the sequence is repeated. It contains all possible states of the register except one forbidden state. The feedback along the LFSR may be either internal or external with no difference in hardware utilization and length of generated sequence. But, data held in LFSR for both configurations at any point of time need not be the same.

LFSR can either be a single input signature register (SISR) or multiple input signature register (MISR). MISR can be used as SISR by making unnecessary Ex-OR gates between flip flops as transparent.

Fig. 1 (a) and (b) shows gate level schematic of SISR and MISR respectively. Here, the remainder stored in SISR or MISR is used as signature. In experiment, register length is taken as 16 bit. But for convenience, in figure 1, it is shown as 4 bit [2].

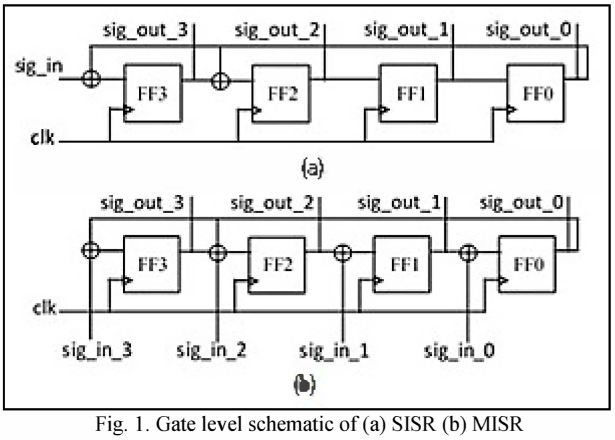

Fig. 1. Gate level schematic of (a) SISR (b) MISR

The proposed secure on-chip comparison technique compares the output of the MISR with the expected response fed into the on-chip comparator from ATE channels. Based on the result of comparison result, PASS/FAIL signature will get generated.

Fig. 2 (a) shows schematic of proposed secure on-chip comparison circuit architecture. Output response compaction block, SR, uses either of *N*-bit signature register shown in Fig. 1 to generate 'sufficiently' unique signature for a given bit stream. SISR is a dedicated signature registers per scan chain whereas MISR, depending on its length, can generate a signature conjointly for scan chains. Also, the golden signature for particular set of test patterns is calculated with knowledge of scan-out bit stream generated by simulator and can be loaded into ATE. The gate level schematic of latch chain is shown in Fig. 2 (b). At the end of test, an Ex-OR operation is performed between test response and expected response stored in latch with the help of sticky comparator. Sticky comparator circuit used in this architecture is taken from [10]. No modification in architecture of sticky comparator is done. Bitwise OR operation is conducted on the result of Ex-OR operation, to identify any mismatch in signatures. This generates final PASS/FAIL test result for that particular test.

As shown in Fig. 2 (a), SO_i are input to SR that is connected to scan-out signals in design and *LSI* is latch chain input used for loading reference signature in latch chain. *s_clk* and *latch_clk* are clock signals for driving signature register and latch chain. The clock used for driving signature register is same as scan clock for DUT. However, any clock signal can be used for loading latch chain. To control the clocking of signature register and latch, separate signature enable *SEn*, and latch enable *LEn*, signals are provided. *latch_clk* is disabled after loading last bit (MSB) of golden signature into latch chain, while *s_clk* is disabled once all test patterns are applied to DUT. This avoids unnecessary transition of signature register after completion of scan-out operation and stabilizes the signature for comparison. In case of multiple self-testing signature-registers in design, latch chains could be further chained by connecting latch output, *LSO*, to *LSI* of next latch chain. By doing this, single *LSI* pin can be used to load all latch chains. Also, OR operation of all *TE* pins can be performed to obtain test result of entire chip.

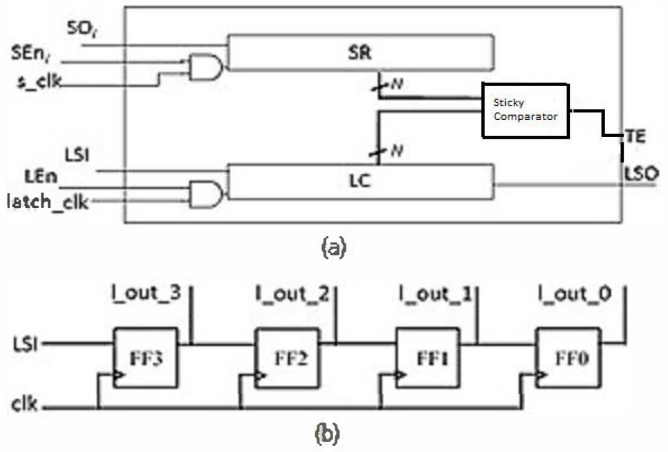

Fig. 2. Schematic of (a) proposed secure comparator and (b) Latch chain

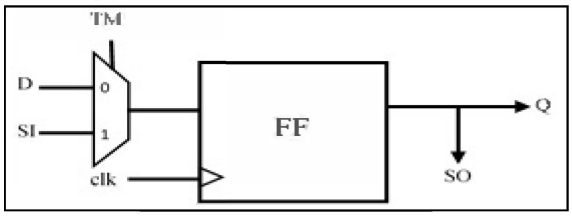

Fig. 3. Scan flip flop used as DFT

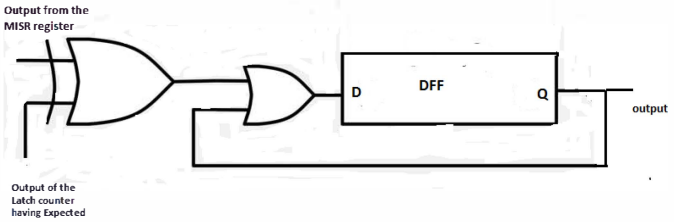

Fig. 4. Architecture of the Sticky comparator

The architecture of sticky comparator is shown in figure 4. Sticky comparator performs the bitwise serial comparison between the output of the MISR and the expected golden response stored in latch chain. The DFF is initially reset. DFF output will be '1' when the comparison fails. The output of the DFF is meaningful in test mode. Based on the output of DFF, result of test is decided.

IV. IMPLEMENTATION

A. Scan Design:

Fig. 3 shows gate level description of conventional scan flip flop used as DFT. The lines *D*, *Q*, and *clk* are the input, output and clock lines respectively. The lines *SI* and *SO* are the input and output for constructing scan path. The output *SO* is connected to *SI* of an adjacent scan flip-flop or a primary output *SCANOUT*. The input *SI* is connected to *SO* of an adjacent scan flip-flop or a primary input *SCANIN*. The line *TM* controls multiplexer for defining mode of operation. When *TM* = 0, the flip-flop is in normal mode of operation. When *TM* = 1, the flip-flop is in scan mode of operation.

B. Design Of Signature Register:

Fig. 2 (a) shows architecture of the proposed signature register with sticky comparator. It uses *LSI* pin to serially shift golden signature into latch chain. Both input patterns and golden response can be fed concurrently to DUT (*SEn = LEn = 1*) and once data is stored into latch, *LEn* signal is disabled (*LEn = 0*). This this does not intervene in application of test patterns at input side. For *p* scan chains, this architecture demands *(p+4)* ATE channels (p channels for scan-in and one each for latch enable, signature enable, latch input and test result). Also, in case of variable-clock scan test, a slow clock may be applied for latching in golden signature. This gives enough confidence for correctness of data stored in latch chain by giving sufficient time for logic to settle at the input of each memory element in scan chain. In case of SISR based system, primary input scan-in can also be used to latch data in latch chain, further reducing a test pin.

The extra area overhead of adding latch chain and sticky comparator is negligible compared with area of whole system. Sticky comparator and latch chain is added to the standard MISR register with an objective to design a countermeasure against scan attacks. MISR based time compaction schemes are proven test data compression mechanisms used to reduce the test time.

There is no need to make changes in standard chip design flow to accommodate this technique. This secure comparator can be synthesized separately and can be added to the design. Also, there is no requirement to change in DFT flow. The standalone module of secure comparator can be inserted in the downstream of the MISR signature generation block for on-chip comparison. So it is easy to include this secure comparator in the design phase.

V. SECURITY AND TEST ISSUES

A. Security:

The countermeasures designed against scan attacks avoid observation of scan flip-flops containing secret information. Secure comparator proposed in this paper is also targeted against scan attacks. Attacker can shift the scan chain data and get the sensitive information easily. In this method, the result of comparison is not accessible at every clock cycle, and it is available at the end of the test vector as in [10]. In [10], output of scan out pin is directly fed into the on-chip comparison circuit. The improvement to [10] is adding MISR based time compaction circuit between scan out and on-chip comparison circuit.

There are two significant advantages of adding MISR based compaction circuit. In [10], the ATE will drive the sensitive data for the on-chip comparison circuit. So it is required to share sensitive data with ATE test engineer or with the Test centre. In the current global supply of semiconductors, it is not recommended to share the confidential data with test centres. In the proposed technique, it is required to share only expected golden signatures, which will get loaded into latch chain with the test centre. This is one security enhancement.

Another significant advantage of this technique is against brute force attacks when the number of scan flip-flops is small in the scan chain. Brute force attack would require $2^{\#SFF}$ attempts. In the proposed method, brute force attack cannot retrieve any sensitive information due to MISR block. The proposed technique is also good defence against attacks proposed in [26].

The disadvantage of this method when compared with [10] is that this technique lacks good diagnostic resolution. BIST and output compaction schemes generally have less diagnostic resolution.

MISR and sticky comparator part of the circuit can be designed in differential power analysis resistant logic style proposed in [29] to have complete defence against any kind of scan attack.

B. Test:

Addition of output response compactor and sticky comparator has no impact on fault coverage. Output of scan chain is compacted for better test time and sticky comparator is introduced as countermeasure against scan attacks. Sticky comparator can be self tested as explained in section III. To conduct experiments relatively larger ISCAS'89 sequential benchmark circuits are selected. The designs are synthesized with TSMC 65 nm technology library using Synopsys design compiler. TSMC8K_Lowk_Conservative wire load model has been considered for interconnects and multiplexed flip-flop as DFT. Also, scan pins in test mode are multiplexed with pins in normal mode with addition of extra test mode pin to switch mode of operation of DUT. In this experiment, multiple scan

chains are used for first five large benchmark circuits, while single scan chain is used for others. To deduce information about delay paths and to check timing violations of design, static timing analysis (STA) has been performed using PrimeTime, Test patterns for testing stuck-at faults and path delay faults are generated using Synopsys ATPG Tool TetraMAX.

The Table I shows test time analysis between the on-chip comparison architecture described in [10] and proposed architecture.

In the Table I, N_{SC} represents number of scan chains, T_{SAF} represents time taken to perform stuck at fault test, T_{PDF} represents time taken to perform path delay fault. Test time is reduced for the proposed MISR based sticky comparator method compared to secure comparator described in [10].

Table II presents the area utilization for the library TSMC 65nm. The area of proposed architecture includes MISR and sticky comparator. The average increase in area for benchmarks circuits is around 500 square microns, which is negligible when compared with overall circuit size.

With the proposed technique there is a significant reduction in test time, which directly impacts the test cost with increase in negligible area.

VI. Conclusions

In this paper, we proposed a new on-chip comparison based design for testability method as a defense against scan chain based side-channel attacks. The proposed technique effectively counters the security attacks. The DFT technique proposed is based on on-chip comparison method which can provide security than previously proposed on-chip comparison schemes. The architectural difference is the inclusion of the MISR signature register between the scan out and sticky comparator. In the proposed method, the two advantages are: there is no requirement to share the confidential information with the test centre, better technique to counter bruteforce attack. Secondly, due to usage of MISR, there is significant reduction in the test time. The experimental results also support our claim.

As a future work, we like to check the proposed technique against differential power analysis attacks as described in [27] and [28].

TABLE I
TEST TIME ANALYSIS

Benchmark Circuits	**Using secure comparator proposed in [10]**			**Using Proposed Architecture with MISR and sticky comparator**		
	N_{SC}	T_{SAF} (ns)	T_{PDF} (ns)	N_{SC}	T_{SAF} (ns)	T_{PDF} (ns)
S35932	16	24900	7200	16	15500	4600
S38584	12	388900	143600	12	260300	97400
S38417	16	52600	109700	16	35700	75700
S15850	10	229100	56400	10	142000	36500
S13207	10	188700	53000	10	136000	36400

TABLE II
AREA UTILIZATION

Benchmark Circuits	***No. of Scan Flip-flops***	***No. of scan chains***	**65 nm TSMC library**	
			Proposed in [10]	***Proposed architecture***
S35932	1728	16	25707.16	26279.21
S38584	1426	12	22425.76	22941.50
S38417	1636	16	22980.88	23652.92
S15850	534	10	7889.12	8676.40
S13207	638	10	8689.00	9476.29

(in square microns)

REFERENCES

[1] M.L. Bushnell and V.D. Agarwal, Essentials of Electronics Testing, Springer, 2000.

[2] Stanley L. Hurst, VLSI Testing: Digital and Mixed analogue/ digital techniques, London, IEE, 1998.

[3] Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Flottes, Rouzeyre and Verbauwhede, "Test versus Security: Past and Present", IEEE transactions on emerging computing-2013.

[4] Stephan Mangard et.al.,"Power Analysis Attacks:Revealing the secrets of smart cards" Springer Science-2007

[5] B.Yang, K.Wu and R.Karri, "Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard", 2004 International Conference on Test , pp 339-344, 2004.

[6] B.Yang, K.Wu and R.Karri, "Secure Scan: A design for test architecture for crypto chips", Computer Aided design of integrated circuits and systems, IEEE transactions on Vol.25, no.10, pp. 2287-2293, 2006.

[7] Y.Liu, K.Wu and R.Karri, "Scan base attacks on linear feedback shift register based stream ciphers", ACM Transactions on Design Automation of Electronic systems, vol.1, no.2, pp 1-15, Mar-2011.

[8] R.Nara, N.Togawa, M.Yanagisawa, and T.Ohtsuki, "Scan-based attack against elliptic curve cryptosystems", in proceedings of the 2010 Asia and South pacific design automation conference-2010, pp 407-412.

[9] Amitabh Das, et.al, "Security Analysis of Industrial Test Compression schemes", IEEE Transactions on computer aided design of integrated circuits and systems, vol.32, No.12, December-2013.

[10] Jean Da Rolt, Giorgio Di Natale et.al, "Thwarting Scan-based attacks on secure ICs with on –chip comparison", IEEE Transactions on VLSI systems, vol.22, No.4, April-2014.

[11] Y.Wu and P.MacDonald, "Testing ASICs with multiple identical cores", IEEE Transactions on computer aided design of integrated circuits, vol.22, no.3, pp.327-336, Mar-2003.

[12] F. Poehl, M.Beck, R.Arnold, J.Rzeha et.al, "On-chip evaluation, compensation and storage of scan diagnosis data", IET Computers and digital techniques, vol.1, no.3, pp.207-212, -2007.

[13] F.Novak and A.Biasizzo, "Security extension for ieee std 1149.1", Journal of electronic testing, vol.22, no.3, pp.301-303, Jun-2006

[14] G.M.Chiu and J.C.M.Li, "A Secure test wrapper design against internal and boundary scan attacks for embedded cores", IEEE Transactions on VLSI systems, vol.20, no.1, pp.126-134, Jan-2012.

[15] A. Das, U. Kocabas, A.S. Sadeghi and I.Verbauwhede, "PUF –based secure test wrapper design for cryptographic SoC testing" Design, Automation and Test in Europe (DATE)-2012.

[16] ARM Ltd. ARM whitepaper on ARM TrustZone. www.arm.com

[17] S.paul, R.Chakraborty and S.Bhunia, "Vim-scan: A low overhead scan design approach for protection of secret key in scan based secure chips", in VLSI Test symposium-2007m 25th IEEE, pp.455-40.

[18] J.Lee, M.Tehranipoor and J.Plusquelllic, "A low cost solution for protecting IPs against scan-based side channel attacks", in VLSI Test symposium-2006.

[19] J.Da Rolt, et.al "A smart test controller for scan chains in secure circuits", in IEEE International online testing symposium-2013.

[20] J.Da Rolt, et.al "New Security threats against chips containing scan chain structures", in Hardware Oriented Security and Trust (HOST)-2011.

[21] G.Senegar, D. Mukhopadhyay and D.R.Chowdhruy, "Secured flipped scan-chain model for crypto-architecture", IEEE transactions on computer aided design on integrated circuits and systems , vol.2, no.11, pp-2080-2084, Nov -2007.

[22] H.Fujiwara and M.E.J.Obien, "Secure and testable scan design using extended de brujin graph", in proceedings of Asia and south pacific design automation conference, 2010, pp.413-418.

[23] D. Hely, F. Bancel, M.L.Flottes and B.Rouzeyre, "Secure scan techniques: A comparison", in proceedings of the IEEE International Symposium on on-line testing -2006.

[24] G. Di Natale, M. Doulcier , M.L. Flottes et.al "Self test techniques for crypto devices", IEEE Transactions on VLSI systems, vol.18, no.2, pp.329-333, Feb-2010.

[25] B.Yang "Design and test for high speed cryptographic circuits", Ph. D Dissertation, New York University-2009.

[26] L.Chunsheng and Y. Huang, "Effects of embedded decompression and compaction architectures on side channel attack resistance", in Proceedings of IEEE VLSI Test symposium, May-2007, pp.461-468.

[27] P.Kocher, J.Jaffe, and B.Jun, "Differential power analysis", in proceedings of International Cryptographic conference-1999, pp. 388-397.

[28] P. Dusart, G. Letourneux, and O. Vivolo, "Differential fault analysis on AES", in Applied Cryptography and Network security, vol. 2846, New York, USA, Springer-Verlag-2003, pp. 292-306.

[29] A. Moradi, T. Eisenbarth, A. Poschmann,et.al "Information leakage of flip-flops in DPA resistant logic styles", in proceedings of IACR. Cryptology, eprint archive, 2008.