HAL
open science

On-Chip Comparison for Testing Secure ICs

Jean da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre

To cite this version:

Jean da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre. On-Chip Comparison for Testing Secure ICs. DCIS 2012 - 27th Conference on Design of Circuits and Integrated Systems, Nov 2012, Avignon, France. pp.112-117. lirmm-00795205

HAL Id: lirmm-00795205

https://hal-lirmm.ccsd.cnrs.fr/lirmm-00795205v1

Submitted on 27 Feb 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On-Chip Comparison for Testing Secure ICs

Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
LIRMM (Université Montpellier II /CNRS UMR 5506)
Montpellier, France
{darolt, dinatale, flottes, rouzeyre}@lirmm.fr

Abstract—**Hardware implementations of secure applications, e.g. cryptographic algorithms, are subject to various attacks. In particular, it has been demonstrated that scan chains introduced by Design for Testability open a backdoor to potential attacks. In this paper we propose a scan protection scheme that provides testing facilities both at production time and during the circuit's lifetime. The underlying principle is to scan-in both input vectors and expected responses, and to perform the comparison between expected and actual responses within the circuit. Compared to regular scan test, this technique has no impact on test quality and no impact on diagnostic of modeled faults. It entails a negligible area overhead and it avoids the use of an authentication test mechanism.**

Keywords – security, testability, scan-based attack, DfT

I. INTRODUCTION

Many aspects of our current life rely on the exchange of data through electronic media. Encryption algorithms are used for guarantying the confidentiality, integrity, and authenticity of these exchanges. These algorithms are implemented on dedicated hardware for performances optimization. After manufacturing, production test allows to sort out good from defective devices, the latter being removed from the production. The quality of the test procedure is primordial for removing devices that could fail in securing the data. Production testing relies on scan-based structural testing because it guarantees high fault coverage and thus product quality.

However, scan implementation open backdoors for security threats. The "Scan attacks" described in [1] and [2] for instance exploit the access offered by scan chain's IOs for retrieving the secret key of an encryption core. These attacks rely on the observability facilities offered by the scan-out operations when the circuit's internal states are related to the secret. The strength of the scan attack resides on the possibility to observe full internal states while monitoring only few nodes, typically the scan-output port(s).

Secure circuits' life cycle varies from other classical products. Classical circuits are designed, manufactured, tested (possibly repaired or re-configured in case of faults), and sold to a system designer who will place the circuit into a board and who will sell the final product to a re-seller, who will commercialize the product to a final client. On the other hand, secure circuits embed confidential information that must be kept undisclosed to unauthorized users. The secret information can be owned by any of the previous actors (i.e., the circuit designer, the manufacturer, the system designer, the re-seller or the final client). This secret can be either hardwired (when set by the circuit designer or manufacturer) or programmed later on using permanent storage elements (e.g., fuses, One Time Programmable memories, EPROM). No matter who introduces the secret into the circuit, the device should be testable at production time and later on, during the whole circuit's lifetime, for maintenance purpose (board-level diagnosis) and possible analysis of feedbacks.

Nevertheless, a straightforward solution and common industrial practice is to physically disconnect the scan chains after production testing. This can be achieved by blowing anti-fuses located at both ends of the scan chains. The only solution for providing full testability afterward is to reconnect the scan chains to IOs. The drawback is that reconnecting the scan chains is also feasible to attackers after the identification of the anti-fuses. Although this procedure requires good skills and specific equipment, the security of the circuit is harmed. The introduction of active shields for preventing micro-probing attacks is a possible countermeasure, but it prevents the test after the scan chains are blown.

Several other solutions have been proposed in literature in order not to disconnect scan chains after manufacturing testing (Section II summarizes the main categories). However, those solutions are either expensive, or not totally secure against new scan attacks. We propose a new DfT method that eliminates the above-mentioned drawbacks. The proposed approach is based on the concept of withholding information. The test procedure consists in providing both test vectors and expected test responses to the Device Under Test (DUT), the comparison with actual responses being performed on chip. The pass/fail comparison result alone is read out from the DUT after application of one test vector.

On-chip comparison of actual and expected test responses has already been explored in other contexts. It allows reducing test data volume in the transfer between tester and DUTs. In [3] for instance, the test mode enables comparisons of identical cores stimulated with identical vectors. It offers an option for observing an accumulated error signature rather than continuous observation, but it requires several (at least 2) identical cores in the design. Another approach has been proposed in [4]. The responses of identical cores are compared with the responses of one core taken as reference, but can also be compared with the expected responses loaded from dedicated scan-inputs. The continuous observation of the comparison result does not provide the security expected in our study. The same remarks can be done for the on-chip comparison mode developed in the wireless multi-site production testing approach described in the patent [5]. In [6], the on-chip

comparison is equipped with a mechanism that stores all relevant scan diagnosis data in a compressed form on the DUT. Failing scan bits are stored into the chip and read after test. This feature must be avoided for preserving confidentiality.

The rest of this paper is structured as follows: Section II presents related works on protection of the scan chain. The proposed solution is presented in Section III. Section IV discusses diagnosis issues and explains how to deal with them. Eventually, Section V draws conclusions on this work.

II. Related Works

Several counter-measures have been proposed to face the scan attacks, while allowing the scan chain access after manufacturing test. Two classes of solutions can be found in literature: the use of dedicated secure test wrappers, and the introduction of hidden functions to obfuscate the real content of scan chains.

Solutions based on the use of secure test wrappers basically implement an FSM with two states: mission mode and test mode. In mission mode, the scan chain cannot be accessed (i.e., the Scan Enable is forced to 0). On the contrary, in test mode the circuit can be tested as a standard scan-based design. The implementation of this type of test wrapper depends on some parameters: how to switch from mission to test mode; what to do when a switch is required; and, possibly, how to further protect the mission mode against invasive attacks.

How to switch from mission to test mode is usually implemented resorting to an authentication protocol. For instance, the solution presented in [7] proposes a security extension for IEEE 1149.1 standard where the test controller must receive a secret wrapper key to enable test mode. More complex wrappers based on challenge-response protocols have been proposed in [8] and [9]. However, secured authentication method requires the implementation of crypto functions into the wrapper and considerably increases the area overhead.

Some papers proposed to trigger a particular event when switching from mission to test mode. [2] proposes the use of a “fake” test key that is used instead of the actual secret key. Internal states observed on scan-out during the test procedure are not related to the secret key anymore in this case. This solution requires additional logic for multiplexing the actual and the “fake” secret key, and the logic to reset the FFs belonging to the scan chain when switching from mission to test mode (otherwise scan chain unloading after switching to test mode allows the observation of an internal state related to the secret key).

If the attacker is able to observe the scan chain even in mission mode (e.g., using micro-probing on the scan enable signal), then the designer must prevent internal state analysis in mission mode. The solution proposed in [10] consists in dynamically and randomly changing the order of segment of the scan chain at every clock cycle. This solution provides a high level of security, however the mechanism for scrambling the data seriously impacts the device area and increases the power consumption at mission mode.

The second class of solution are less expensive and do not require any form of secure wrapper. The basic idea of this class of solutions is to implement a secret function within the scan chain to obfuscate its content. The tester knows the particular hidden procedure implemented in the design and test data are first processed before being compared to expected data. In [11], inverters are inserted in the scan chain, providing bit flipping while the data are scanned out. Authors in [12] propose to add XORs networks to the scan chain, providing linear combination of test data at the scan out instead of test data itself. However, these solutions assume that there is no way for the attacker to get information on the scan chain implementation (security by obfuscation). Besides, it has been shown that these solutions prevent scan-attacks such as the ones presented in [1] and [2] but are susceptible to more recently published scan attacks [13].

More recently, advanced DfT schemes including response compaction and X-masking techniques have been discussed for acting as countermeasures [14]. The expected role of the compactor is also to scramble the test data in such a way that it would be impossible to retrieve the test responses caught in the scan chain, and thus the secret related to these data. Unfortunately, recently proposed attacks [7] circumvent this type of protection.

III. Proposed Solution

All the scan attacks proposed till now [1-2, 3] rely on the possibility for the hacker to observe functional intermediate states of the circuit by means of the scan chain. Therefore, countermeasures consist in blocking the observation of the scan chain outputs.

The basic approach proposed in this paper is based on the comparison of the actual responses against the expected ones within the chip boundaries instead of scanning out the actual responses and doing the comparison within the external tester.

Figure 1 illustrates a standard test scheme.

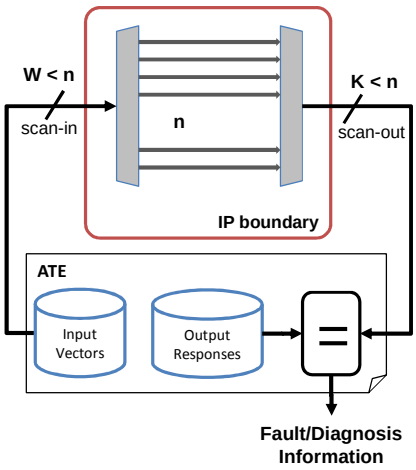

Figure 1: Standard Test Scheme

The input vectors are loaded into the scan chains via the W scan-in pins (W<n). The W signals are decompressed into n signals (one for each scan chain), and the circuit runs one functional clock cycle. Then, the

response vector is compacted into K output signals and scanned out via scan-out pins (K<n). The external tester compares those values with the expected responses. Depending on the observed differences, the ATE is able to verify the presence of faults. Further analysis of eventual erroneous responses allows identification of fault(s) that may generate the observed error.

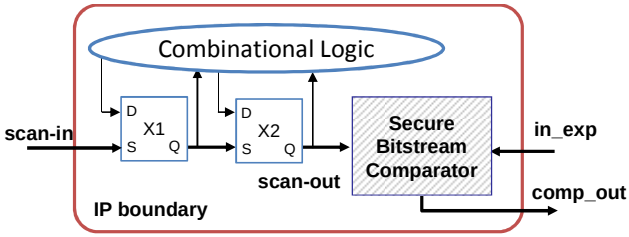

Figure 2: Basic Solution

Figure 2 shows the basic principle for on-chip comparison of one scan chain. Nevertheless, this scheme can be also used in presence of multiple scan-chains and test data compaction mechanisms. As for the standard test scheme, an input vector is loaded into the chip, a clock cycle is run while the circuit is in normal mode and then the response (several bits) is captured into the scan chains. Instead of shifting the response out of the chip, the external tester scans-in the expected responses using an *in_exp* pin that would have been used as Scan-Out in the standard scheme. The actual test response is compared on-chip, pair-wise, against the expected one. In particular, for each bit shifted-out from a scan chain, the related expected response bit is scanned-in through the *in_exp* pin. After comparison of all bits captured in the scan-chain, and only at that moment, the additional output pin *comp-out* is set to 1 if and only if the whole response vector matched the expected one, otherwise *comp-out* is set to 0.

In order not to allow any successful scan attack, the comparison between actual and expected responses must be kept hidden until all flip-flops belonging to the scan chain are compared. Otherthewise, an attacker could devise the content of the scan chain by applying the sequence "000…00" on the *in_exp* pin.

The serial *Secure Bitstream Comparator* is depicted in Figure 3. The *Counter* allows the observation of the overall test result only at the end of a scan cycle. It is initialized to 0 when the Scan Enable switches from 0 to 1, and it rises up the Terminal Count (TC) signal after L clock cycles, where L is the number of scan-FFs in the chain.

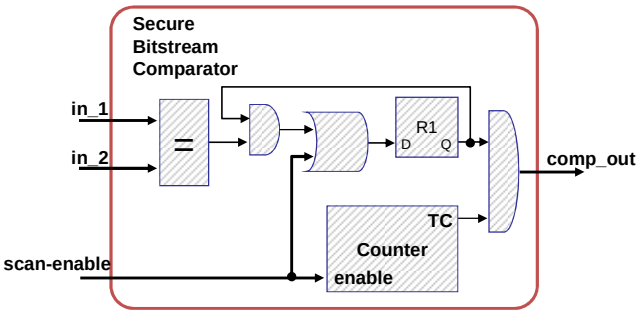

Figure 3: Secure Bitstream Comparator

To sum up, a serial comparator is composed of one FF for the *R1* and $\log_2(L)$ FFs for the counter, 2 AND gates and 1 NXOR gate for the 2-bit comparison.

Next subsections will analyze the security enhancements provided by this solution and discuss the impact of the proposed approach in terms of additional costs and impact on the testability.

A. *Security Analysis*

The role of the proposed test controller is to avoid the observability of FFs containing secret information. If the comparison were accessible at each clock cycle instead of each scan cycle as proposed, an attacker would easily observe the scan chain content by shifting in "000…000" on the *in_exp* pin. Each bit-comparison would then confirm that the actual bit was 0 (if *comp_out*=1) or 1 (if *comp-out*=0). With the proposed comparison per scan cycle, the only way to retrieve the information related to the sensitive data, is to try the whole set of expected responses until a positive answer is obtained from the *comp_out* signal (i.e. brute-force attack). For the basic proposed solution (see Figure 2) the comparator takes into account all the FFs of the design. Thus, for L scan-FFs, an attack would take 2^L attempts.

It must be noticed that side-channel attacks (like power analysis [15]) could be used to sense whether the 2-bit comparator has changed its state. This would make the response vectors visible to the attacker. However, several effective and low-cost countermeasures have been proposed in order to face this issue (e.g. [16]).

B. *Area Ovehead*

In order to discuss the area overhead and impact on testability we consider a comprehensive scenario (see Figure 4) where the DUT has n scan chains, W (smaller or equal to n) input test channels, an eventual test data decompressor (from W to n), an eventual test data compactor from n to K (K≤n). We also consider that the K compacted output scan chains are composed of K_p (<K) chains that do not store any confidential data, and K_s (=K–K_p) chains that contain secret information.

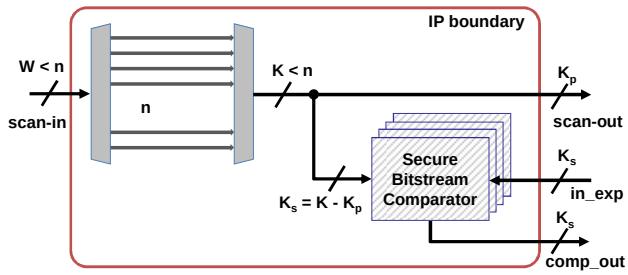

Figure 4: Solution for multiple Scan Chains

The area overhead is shown in Table I, where it is divided in two subcircuits: the embedded counter and the rest of the SBC. The embedded counter can be shared for several SBCs while the rest of the SBC must be inserted for K_s outputs. We assumed scan chains with length up to 256 flip-flops, thus the counter has 8 bits. The design was synthesized with AMS 0.35µm digital library cell. The

second and third columns show the area in nm and gate equivalent, while the fourth one presents the area overhead compared to a small symmetric cipher (Khazad [17], with 9879 GEs). As it can be seen, the area overhead introduced by the test wrapper is negligible, even for a large number of K_s.

TABLE I. AREA OVERHEAD

Secure Bistream Comparator	Area *(nm²)*	Area *(GE)*	Area Overhead*
Counter (8-bit)	4770.8	87.37	0.88%
Comparator	663.2 * K_s	12.14	0.12%

**Applied to Khazad symmetric cipher [17]*

Unluckily, this solution requires K_s extra *comp_out* pins in order to observe all the comparison results. This problem can be solved by using bidirectional pins as shown in Figure 5. Each original *in_exp* pin is replaced by a bidirectional one and used for transmission of the comparison result. Usually, pads with input direction or input/output have the same area, thus this technique does not increase the pad area.

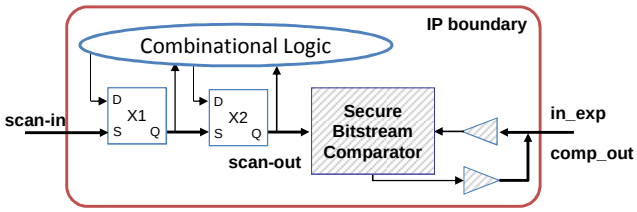

Figure 5: Bi-directional test pins

During the shift operation, the pin is set as input and used by the tester to feed the circuit with the expected responses. In the capture operation the pad is activated as output and releases the previous comparison result. Thus no extra clock cycle is required to communicate the response.

C. Design Flow

Regarding the design flow, the solution may be easily inserted after the DfT phase. The Secure Bitstream Comparator IP can be connected to the K_s test outputs.

D. Impact on Testability

Concerning the test coverage, the proposed solution do not impact test results in the sense that every test response is compared with the expected one, as in a standard test scheme. Therefore, the achievable fault coverage is not altered. Concerning the testability of the wrapper itself, it may be achieved by means of functional test. For instance, some input vectors may be loaded into the design and the response could be compared with good and bad responses. This would test the controller and the serial comparator circuits since they have simple logic.

Test time is not increased since the expected responses are scanned-in at the same time that the next input vector is scanned-in on SI pins.

The presence of unpredictable values in the scan flip-flops may corrupt the comparison value, the same way it would corrupt a design tested by BIST. These X's can be handled using several solutions proposed in the literature and implemented by industrial DfT tools [18]. However, an additional issue must be addressed: the diagnostic of eventual "fail" responses. This solution allows the tester to detect the presence of faults, but the diagnostic passes from bit-wise observable to vector-wise observable. This reduces the diagnosis resolution as shown in Section IV. A new procedure to recover the faults that cause the mismatch is presented in Section IV though.

IV. DIAGNOSIS ISSUES

In the standard test scheme, faults can be directly observed at every bit stored in the scan chain, while in the proposed solution a single test result (pass/fail) is related to the whole test response. In order to analyze the diagnostic resolution loss, we applied the proposed countermeasure to following benchmarks: ISCAS85, ISCAS89 and ITC99. For each circuit we inserted a single scan chain and then we created two versions of the circuit, one with the standard test scheme (called Bit-Wise Observation) and a second one with the proposed countermeasure (called Vector-Wise Observation). TetraMAX ATPG generated the input vectors and the list of collapsed faults for each version of the circuits. Then, using Lifting [19], we simulated the test procedure and created the fault dictionary. From the fault dictionary we analyzed the diagnostic resolution loss.

Figure 6 gives the average, over all benchmark circuits, of the percentage of faults for each diagnosis resolution. Diagnostic resolution N contains the faults for which diagnostic cannot distinguish between N suspect faults. As it can be seen, for the Bit-Wise Observation (standard test procedure) in average, 95.20% of the faults can be solely diagnosed. 4.80% of faults have a diagnosis resolution of 2. With the proposed solution (Vector-Wise Observation), the group of faults solely diagnosed is reduced to 68.37%, i.e. a loss of 28.19% compared to the Bit-Wise Observation. We did the same experiment with another set of test patterns for which each fault is detected

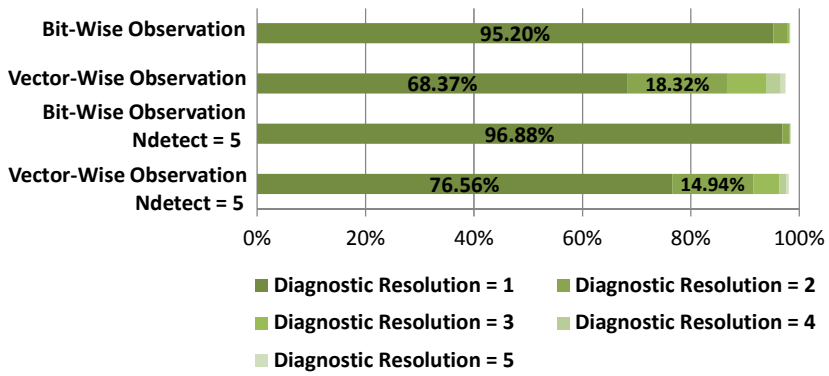

Figure 6: Diagnostic resolution loss

by 5 patterns (Ndetect=5). Doing so, the diagnosability loss is reduced to 20.98%, meaning that using the

proposed solution almost 80% of the faults are still detected with the same resolution.

For more precise resolutions, the diagnostic procedure can be modified as follows to achieve 0% of loss. For each vector that shows an error on *comp-out*, the circuit must be stimulated again, not with the expected pass response as in the first phase (test), but using expected faulty responses (diagnosis). All possible wrong responses are used as expected result for the same input vector. For instance, the vector V1 tests the faults F1 and F2. R1 is the expected response in presence of F1, R2 is the expected response in presence of F2 (simulation results). The vector V1 is applied at the input with R1 as expected result, and then with R2. If the fault F1 is responsible for the error, the comparison in the first case matches, otherwise F2 is responsible for the error. The diagnosis resolution is the same as in a standard test scheme in this case. This procedure only entails an additional time for diagnostic purpose.

However, the proposed procedure is only valid if the errors observed are caused by faults that were previously modeled. Not-modeled faults result in unknown test responses and thus cannot be diagnosed using expected test responses. Moreover, there is no way to know the faulty responses stored in the scan chain in presence of such faults due to the security feature that hides the scan chain contents. The following sub-sections describe alternatives for limiting this diagnostic loss.

A. Rerouting

The first solution is to build scan chains containing sensitive FFs only. The on-chip comparison is then only applied to these chains. The diagnosis precision of the non-secure part is kept unchanged while the diagnosis of the secure part may be reduced. This solution supposes a controllable scan chain routing and multiple scan chains.

B. Ad-hoc

The solutions proposed previously in this paper may be applied after building the scan chains, and they can be applied also for IP cores. However, the same underlying principle may be used during the design of the circuit and only to the sensitive data.

As before, the content of the FFs are compared to the expected response within the circuit, however, this comparison is limited to sensitive FFs only, whatever their position in the scan chains (there is no dedicated “secure” scan chains as before). Differently from before, the expected responses of the sensitive FFs are loaded inside the circuit by means of the regular scan-in pins and stored in additional FFs denoted RFFs (redundant). When the expected response matches the actual one, the content of the scan-chain is scanned-out as in regular scan. There is no security issue in this case. In the opposite case, sensitive FFs are reset during the scan-out operation. Thus, no sensitive information can leak through the scan chain observation.

This technique is depicted in Figure 7. XFFs contain non-sensitive information while SFFs contain secret information. In order to compare the test responses, there are as many RFFs as SFFs. When the *scan-enable* is asserted, input vectors are loaded into the scan chains and, at the same time, previous scan chain content is scanned out. The input bitstream contains the test pattern for both X and S FFs, as well as the expected response for S FFs in the RFF positions. During the capture clock cycle, RFFs keep their state, while XFFs and SFFs are updated according to the combinational logic. After the capture cycle, RFFs and SFFs are compared and the result is stored in an extra DFF. This comparison value is then used to erase or not the secret information when scanning out. A rise-edge detector on scan-enable synchronizes the comparison between RFFs and SFFs and the shift-out operation. An additional AND gate is added to filter the erase signal.

According to the simulation waveform in Figure 7, the presence of sequential elements in the rise-edge detection and the comparison introduces a delay. For this reason, the erasing circuitry, i.e., the black AND gates inserted in the scan path (see Figure 7), is inserted one position right to each SFF.

In terms of testability, the fault coverage is not harmed for the same reason stated in Subsection III.B. Another advantage of this technique is that the diagnosis of the non-sensitive part of the design is not impacted.

However, the overall test time is increased by S clock cycles per scan cycle where S is the maximal number of sensitive FFs over one scan chain, because of the insertion of RFFs. For multiple chains the extra FFs may be distributed over all the scan chains, reducing the impact on the test time.

V. CONCLUSIONS

In this paper we have proposed a novel DfT technique for scan design to ensure security without relying on the use of costly test infrastructures for switching from mission to test modes. The proposed approach is based on the concept of withholding information. The idea is to enhance the classical on-chip test data comparison scheme. Both input vectors and expected responses are scanned into the DUT and the comparison between expected and actual responses is done at test vector level. It does not provide information on the value of each individual scan bit for security purposes.

Compared to regular scan test, this technique has no impact on test quality and no impact on diagnostic of modeled faults. Moreover, it does not impede test activities at the circuit’s lifetime. Solutions have also been provided in order to handle possible unknown values in the test responses and limit possible diagnostic loss to sensitive circuit parts. The technique entails a negligible area overhead and it does not require the designer to be particularly aware of security issues. The method can be applied after building the scan chains and therefore it can be applied for IP cores as well.

REFERENCES

[1] Bo Yang; Kaijie Wu; Karri, R.; , "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, Oct. 2006

[2] Bo Yang; Kaijie Wu; Ramesh Karri; , "Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard," *Test Conference, 2004. Proceedings. ITC 2004. International* , pp. 339- 344, 26-28 Oct. 2004

[3] Yuejian Wu; MacDonald, P.; , "Testing ASICs with multiple identical cores," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on* , vol.22, no.3, pp. 327- 336, Mar 2003

[4] Balakrishnan, K.J.; Giles, G.; Wingfield, J.; , "Test Access Mechanism in the Quad-Core AMD Opteron Microprocessor," *Design & Test of Computers, IEEE* , vol.26, no.1, pp.52-59, Jan.-Feb. 2009

[5] Patent US-2011-0244814-A1, http://www.google.com/patents/about/System_and_Method_for_Wirelessly_Testing.html?id=itP0AQAAEBAJ

[6] Poehl, F.; Beck, M.; Arnold, R.; Rzeha, J.; Rabenalt, T.; Goessel, M.; "On-chip evaluation, compensation and storage of scan diagnosis data," *Computers & Digital Techniques, IET* , vol.1, no.3, pp.207-212, May 2007

[7] Chiu, G.-M.; Li, J. C.-M.; , "A Secure Test Wrapper Design Against Internal and Boundary Scan Attacks for Embedded Cores," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on* , vol.20, no.1, pp.126-134, Jan. 2012

[8] Rosenfeld, K.; Karri, R.; , "Attacks and Defenses for JTAG," *Design & Test of Computers, IEEE* , vol.27, no.1, pp.36-47, Jan.-Feb. 2010

[9] Clark, C.J.; , "Anti-tamper JTAG TAP design enables DRM to JTAG registers and P1687 on-chip instruments," *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on* , pp.19-24, 13-14 June 2010

[10] Hely, D.; Flottes, M.-L.; Bancel, F.; Rouzeyre, B.; Berard, N.; Renovell, M.; , "Scan design and secure chip [secure IC testing]," *On-Line Testing Symposium, 2004. IOLTS 2004. Proceedings. 10th IEEE International* , pp. 219- 224, 12-14 July 2004

[11] Sengar, G.; Mukhopadhyay, D.; Chowdhury, D.R.; , "Secured Flipped Scan-Chain Model for Crypto-Architecture," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on* , vol.26, no.11, pp.2080-2084, Nov. 2007

[12] Fujiwara, H.; Obien, M.E.J.; , "Secure and testable scan design using extended de Bruijn graphs," *Design Automation Conference (ASP-DAC), 2010 15th Asia and South Pacific* , pp.413-418, 18-21 Jan. 2010

[13] Da Rolt, J.; Di Natale, G.; Flottes, M.-L.; Rouzeyre, B.; , "New security threats against chips containing scan chain structures," *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on* , pp.110, 5-6 June 2011

[14] Chunsheng Liu; Yu Huang; , "Effects of Embedded Decompression and Compaction Architectures on Side-Channel Attack Resistance," *VLSI Test Symposium, 2007. 25th IEEE* , pp.461-468, 6-10 May 2007

[15] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. 1999. "Differential Power Analysis," In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology* (CRYPTO '99), Springer-Verlag, London, UK, pp. 388-397.

[16] Moradi, A., Eisenbarth, T., Poschmann, A., Rolfes, C., Paar, C., Shalmani, M.T.M., Salmasizadeh, M.: "Information Leakage of Flip-Flops in DPA-Resistant Logic Styles," Cryptology ePrint Archive, Report 2008/188 (2008)

[17] P. Barreto, V. Rijmen, "The Khazad legacy-level block cipher," *First open NESSIE Workshop*, Leuven, 13–14 November 2000, 15 pages.

[18] Patel, J.H.; Lumetta, S.S.; Reddy, S.M.; , "Application of Saluja-Karpovsky compactors to test responses with many unknowns," *VLSI Test Symposium, 2003. Proceedings. 21st* , pp. 107- 112, 27 April-1 May 2003

[19] Bosio, A.; Di Natale, G.; , "LIFTING: A Flexible Open-Source Fault Simulator," *Asian Test Symposium*, 2008. *17th*, pp.35-40, 24-27 Nov. 2008

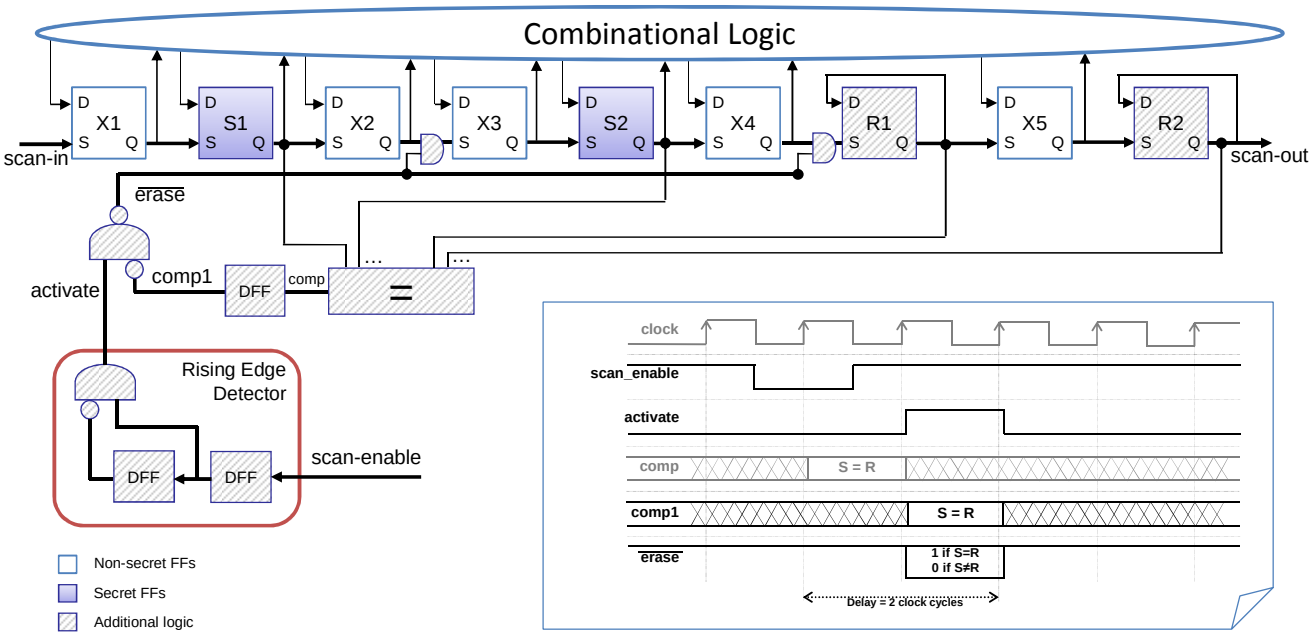

Figure 7: Proposed solution applied locally