Secure Scan Design with a Novel Methodology of Scan Camouflaging

Srisubha Kalanadhabhatta[1], Kiran Kumar Anumandla[1], Saqib Khursheed[2] and Amit Acharyya[1]
[(1)] *Department of Electrical Engineering, IIT Hyderabad, India*
[(2)] *Department of Electrical Engineering and Electronics, University of Liverpool, UK*

***Abstract*—Scan based attacks are the major security concerns of a design. These attacks are majorly employed to understand the camouflaged logic during reverse engineering. The state-of-the-art techniques like scan chain scrambling hinder accessibility of scan chains, but are prone to layout level reverse engineering attacks. In the proposed methodology, the scan design is secured by adding an extra scan input port (DSI) to the flipflop using dummy contacts, which ensure that DSI cannot be distinguished from SI port even with layout based reverse engineering techniques. Dummy scan chain connections are introduced in the design by connecting DSI port to the nearby flipflop Q output port. Our proposed method can withstand Reset-and-scan attack, Incremental SAT-based attack and the recent ScanSAT attack. The performance of this concept is measured in terms of frequency and total power consumption on IWLS-2005 benchmark circuits having up to 1380 flipflops with 40nm technology library. The delay is effected by a maximum of 2.2% with 50% obfuscation without any impact on power, pattern generation time and scan test time.**

***Index Terms*—Scan Chain, Hardware Security, Camouflage, Obfuscation, Dummy Contacts, SAT**

I. Introduction

TEST and security are the most critical requirements for a trusted IC design. Scan test structures are generally inserted in the design with an intent to increase testability [1] which are exploited in scan based attacks to break security. The motto of the attack is either to break the security of symmetric-key or public-key cryptography [2]- [4] or to decode the camouflaged combinational logic [5]. In this paper, we focus on the scan based attacks to decode the camouflaged combinational logic. Camouflaging, a layout based technique where different logic functions can be implemented by look-alike cells [6] or obfusgates [7], is widely used to enhance security of a design. In SAT-based attack, [8], camouflaged standard cells [6], obfusgates [7] or the transformable interconnects [9] are represented as a multiplexer based model having all required combinations. The functionality of the circuit is determined by finding the select lines of multiplexer by controlling and observing its ports with the help of scan chains. To overcome SAT attack, inter flipflop connections can be obfuscated by using RNG based scrambling techniques [10]. But, the RNG can be bypassed or removed and fixed pattern can be inserted when an incorrect sequence is used. Locking muxes are inserted in the recently proposed key based Encrypt Flipflop method [11]. However, as reported in [11], this method is vulnerable to Reset-and-scan attack. ScanSAT attack [12], transforms scan obfuscated circuit into its logic locked version and applies a variant of SAT based attack [8] to extract the secret key by controlling/observing the scan-in/scan-out pin. The scan chain connections obtained may not exactly match the actual scan connections. A technique to reverse engineer without the use of scan chains [13], is effective only if the ratio of the primary IOs to the Scan flipflops is reasonably large which is not applicable for realistic circuits.While [13] takes on a goal of attacking with no scan access, such attacks need further development to be successful on realistic designs.

In view of above, we introduce a novel methodology to secure the design from the state of the art scan based attacks. The key contributions of the paper are

- The proposed methodology secures the design from the state of the art techniques like Incremental SAT, ScanSAT and Layout level Reverse Engineering attacks.
- The proposed methodology has least impact on the design in terms of performance that includes delay, power and pattern generation time.

II. Proposed Methodology

In the proposed countermeasure, scan camouflaging flipflops are created by adding a second scan input pin to the scan flipflop. One of the scan inputs is connected with actual contact and is referred to as SI. Another scan input is connected with dummy(no) contact and is referred to as DSI. Hence, although two scan inputs are present, only one of them is internally routed and connected to flipflop output. Figure 1 shows the layout of scan camouflaging flipflop. Two different versions of scan camouflaging flipflops have to be created by interchanging the locations of SI and DSI. After scan stitching, selected scan flipflops are converted into one of these two versions of scan camouflaging flipflops. Extra scan connections are made by connecting the DSI of these flipflops to the outputs of nearby flipflops. Consider Figure 2 where ten flipflops are stitched into two scan chains with five flipflops in each chain. Chain1 consists of flipflops A, B, C, D and E and chain2 consists of flipflops F, G, H, I and J. Flipflops B, C, D, E, G, H, I and J are converted into scan camouflaging flipflops. Instead of adding a new port DSI, for ease of representation, the dummy scan connections on these flipflops B, C, D, E, G, H, I and J are shown in blue dotted lines. To differentiate between the actual scan connections and dummy

This work is partially supported by Ceremorphic India Pvt. Limited, NPDF, SERB, Government of India (GOI) and SMDP-C2S, MEITY, GOI.

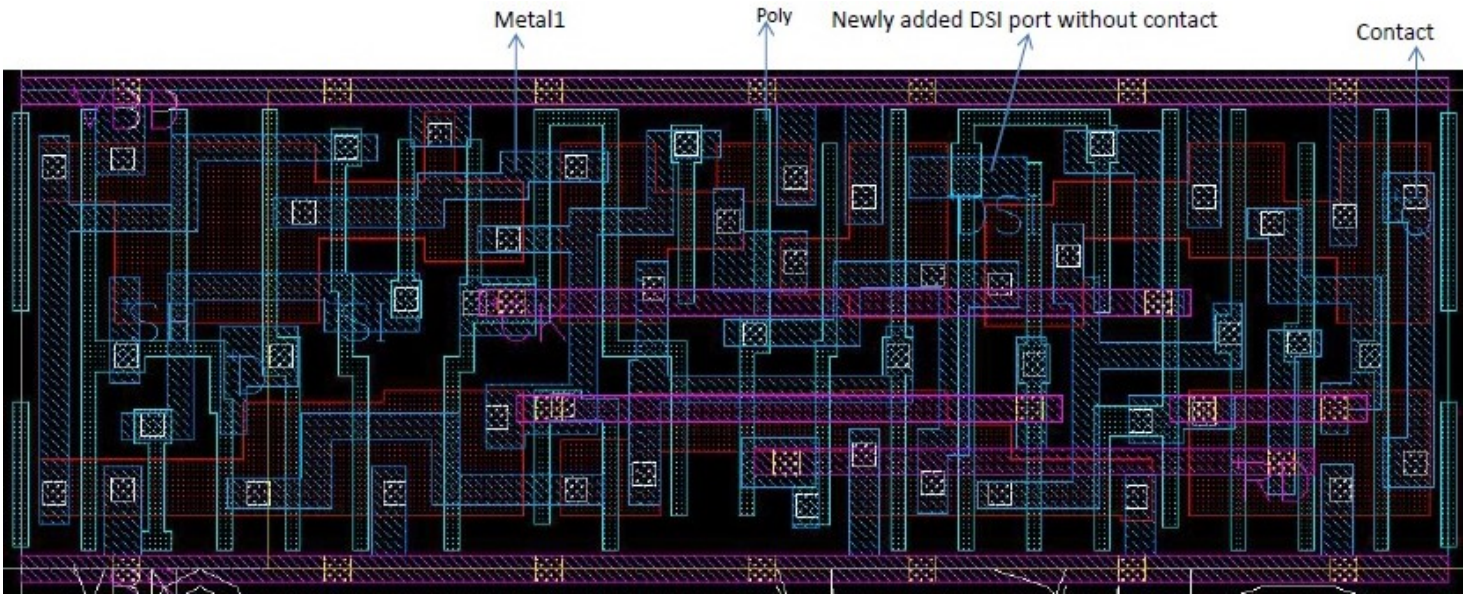

Fig. 1. Layout of Proposed scan camouflaging flipflop

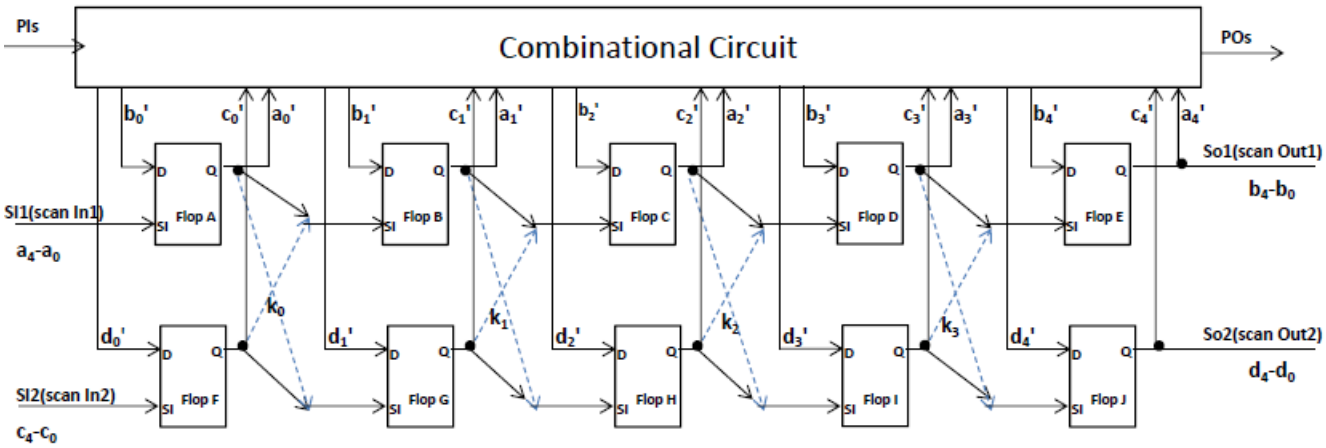

Fig. 2. Protection using Proposed methodology

scan connections, the attacker has to differentiate between SI and DSI of the scan camouflaging flipflops. For ascertaining this, the attacker has to partially etch the metal layers from top-down using anisotropic techniques like reactive-ion etching. While applying these techniques, by the time the attacker comes to the bottom layers, the dummy contacts are almost eroded by the chemicals. Attacker cannot distinguish if a broken contact is because of chemical erosion or camouflaging [14] - [15]. Hence, proposed technique makes it difficult to delayer the device and decode the scan architecture even with image processing based reverse engineering techniques. The cost and effort that is required to decode the scan architecture outweighs the advantage of reverse engineering. IWLS-2005 benchmark circuits are implemented using these flipflops. Results are analyzed for understanding the impact on delay, power, pattern generation time and scan test time. To further increase the complexity, by including the proposed methodology in the form of an automated Computer Aided Design tool, the scan camouflaging flipflops configuration can be made different for different devices. In such a case, although the attacker does reverse engineering and understand the logic of one device, the scan camouflaging flipflops of other devices cannot be ascertained. But, having different layout for each device is not a feasible solution. Hence, there can be few different versions of the device and they all can be manufactured on the same wafer.

TABLE I
POSSIBILITIES WITH 2 SCAN CHAINS HAVING 4 SCAN CAMOUFLAGING FLIPFLOPS IN EACH CHAIN

Possibility	Chain1	Chain2
1	SI1-A-B-C-D-E-SO1	SI2-F-G-H-I-J-SO2
2	SI1-A-G-C-D-E-SO1	SI2-F-B-H-I-J-SO2
3	SI1-A-B-H-D-E-SO1	SI2-F-G-C-I-J-SO2
4	SI1-A-G-H-D-E-SO1	SI2-F-B-C-I-J-SO2
5	SI1-A-B-C-I-E-SO1	SI2-F-G-H-D-J-SO2
6	SI1-A-G-C-D-E-SO1	SI2-F-B-H-I-J-SO2
7	SI1-A-B-H-I-E-SO1	SI2-F-G-C-D-J-SO2
8	SI1-A-G-H-I-E-SO1	SI2-F-B-C-D-J-SO2

A. Investigating the effect of Incremental SAT-based attack on the design having scan camouflaging flipflops

Incremental SAT-based attack requires the understanding of scan architecture and its full controllability and observability. Attacker understands the scan architecture from the images that are obtained during reverse engineering [16]. Our proposed methodology adds confusion because of dummy scan input ports. Although layout information can be obtained from images, the actual scan architecture cannot be ascertained as there would be confusion on which port is dummy scan input.

Consider the scan camouflaging flipflop network as shown in Figure 2. The scan camouflaging connections are named as k0, k1, k2 and k3. In this circuit, with two scan chains and four scan camouflaging flipflops per chain, the total number of possibilities to create confusion is eight as depicted in Table I. Unless the attacker finds out which of the camouflaging connections, k0, k1, k2 and k3 are valid, he/she will not be able to find out which signal is getting connected to the combinational logic input and to what scan out the combinational logic output is connected. Similarly, for 4 scan chains and 4 scan camouflaging flipflops per chain, the total number of possibilities to create confusion is sixteen. As there is confusion both in controlling and observing the camouflaged combinational circuit, even two camouflaging flipflop combinations that create confusion (one for controllability and the other for observability) would make it difficult to apply SAT-based attack. Hence, the camouflaged combinational circuit cannot be decoded using incremental SAT-based attack in the presence of scan camouflaging flipflops.

B. Investigating the effect of ScanSAT attack on the design having scan camouflaging flipflops

ScanSAT [12] helps transforming any obfuscated sequential logic into logic locked problem with keys. The logic locked problem can be resolved using SAT-based attack [8]. The relation between scan In1 ($a_4 - a_0$) and the pattern delivered into the scan chain1 ($a'_4 - a'_0$) can be formulated as

$$a'_0 = a_0 \tag{1}$$

$$a'_1 = a_1\overline{k_0} + c_1k_0 \tag{2}$$

$$a'_2 = a_2\overline{(k_0 \oplus k_1)} + c_2(k_0 \oplus k_1) \tag{3}$$

$$a'_3 = a_3\overline{(k_0 \oplus k_1 \oplus k_2)} + c_3(k_0 \oplus k_1 \oplus k_2) \tag{4}$$

$$a'_4 = a_4\overline{(k_0 \oplus k_1 \oplus k_2 \oplus k_3)} + c_4(k_0 \oplus k_1 \oplus k_2 \oplus k_3) \tag{5}$$

Similarly, for scan chain2 ($c'_4 - c'_0$) can be represented in terms of ($c_4 - c_0$) by replacing c and a with a and c respectively in the equations (1) - (5)

The relation between scan chain1 captured response pattern ($b'_4 - b'_0$) and the observed pattern at scan out1 ($b_4 - b_0$) can be formulated as

$$b_4 = b'_4 \tag{6}$$

$$b_3 = b'_3\overline{k_3} + d'_3k_3 \tag{7}$$

$$b_2 = b'_2\overline{(k_2 \oplus k_3)} + d'_2(k_2 \oplus k_3) \tag{8}$$

$$b_1 = b'_1\overline{(k_1 \oplus k_2 \oplus k_3)} + d'_1(k_1 \oplus k_2 \oplus k_3) \tag{9}$$

$$b_0 = b'_0\overline{(k_0 \oplus k_1 \oplus k_2 \oplus k_3)} + d'_0(k_0 \oplus k_1 \oplus k_2 \oplus k_3) \tag{10}$$

Similarly, for scan chain2 ($d_4 - d_0$) can be represented in terms of ($d'_4 - d'_0$) Similarly, for scan chain2 ($c'_4 - c'_0$) can be represented in terms of ($c_4 - c_0$) by replacing b and d with d and a respectively in the equations (6) - (10). There are ten equations to find out four variables and hence, the equations can be resolved and the values of k0, k1, k2 and k3 can be ascertained. As mentioned in [8], while the overall circuit produced by SAT is guaranteed to be functionally equivalent to the obfuscated circuit, there is no guarantee it will match the obfuscated circuit on a gate-by-gate basis. Hence, the scan connections that are obtained from scanSAT cannot be guaranteed to be correct on per connection basis. Considering the circuit as shown in Figure 2, unless we find values of k0, k1, k2 and k3 combinations as listed in Table I, we cannot ascertain the connections between scan ports and combinational logic ports. Hence, ScanSAT may not exactly provide the clarity of the connections required.

When the number of scan camouflaging connections are significantly larger as in case of scan compression, the number of equations that can be formulated would be very less compared to the variables to be solved. For example, for a compression ratio of 2 for the same circuit, we can have a maximum of five equations for four scan camouflaging flipflop connections. For a compression ratio of 4 for the same circuit, we can have a maximum of five equations for eight scan camouflaging flipflop connections, which cannot be resolved. Number of equations are dependent on the number of flipflops in the scan chain where as the number of scan camouflaging connections depend on the number of flipflops. As the compression ratio increases, the problem becomes more complex and cannot be resolved using scanSAT.

III. Experimental Setup and Results

Logical synthesis is carried out with the Synopsys Design Compiler using GF 40lp standard cell libraries. Scan stitching is done on the synthesized netlist using DFT compiler to have 10 scan chains for each design. Floorplan and placement steps are carried out in Cadence Encounter. The flipflops that have to be camouflaged are replaced with the flipflops having DSI port. The DSI of these flops is connected to Q port of the nearby flipflops. Clock Tree Synthesis and Routing are done on this netlist in Encounter tool. On the routed netlist, Static Timing Analysis is carried out using PrimeTime and Power Analysis is done using PT-PX. The proposed idea with 50% obfuscation is implemented on six IWLS-2005 circuits in total and implementation results are shown in Table II. It is observed that there is 13% to 25% increase in net length, an impact of 0.7% to 2.2% on frequency and 0.05% to 0.38% on power consumption compared with the original circuit implementation. As there is no change in the logical netlist,

TABLE II
BENCHMARK CIRCUIT ANALYSIS WITH THE PROPOSED METHODOLOGY

		Original Statistics (Without Obfuscation)			Proposed Methodology (50% Obfuscation)			Difference		
Circuit	**No.of Flops**	**Frequency F(MHz)**	**Total power P(mW)**	**Net length L(μm)**	**Frequency F(MHz)**	**Total power P(mW)**	**Net length L(μm)**	**ΔF (%)**	**ΔP (%)**	**ΔL (%)**
usb_phy	98	473	0.34	4331	464	0.34	5041	1.9	0.23	16.4
sasc	116	458	0.40	5449	448	0.40	6351	2.2	0.05	16.6
des	190	188	0.64	19948	184	0.64	22667	2.2	0.34	13.6
spi	229	188	0.24	20429	183	0.24	24223	2.2	0.38	18.6
s38584	1380	193	2.16	204335	190	2.17	256476	1.7	0.37	25.5
wb_conmax	818	147	0.84	400104	146	0.85	452279	0.7	0.37	13.0

TABLE III
COMPARISON WITH EXISTING TECHNIQUES

Metrics	**Scrambling [10]**	**Encrypt Flipflop [11]**	**Proposed Methodology**
Type of countermeasure	Obfuscation based	Obfuscation based	Obfuscation based
Layout level reverse engineering	Vulnerable	Not Vulnerable	Can withstand because of dummy contacts
Reset-and-scan attack	Not Vulnerable	Vulnerable [11]	Not Vulnerable

there would be no impact on pattern generation time and test time.There would be slight increase in the area with the addition of dummy port if the requirement of having same electrical and timing characteristics has to be met. We could not quantify the area increase because of the unavailability of such a flipflop from the foundry. But it is expected to be very small and depends on the % obfuscation. The performance metrics of the proposed methodology are compared with the state of the art countermeasures for scan based attacks like Encrypt flipflop [11] and Scrambling [10] as shown in Table III. The state of the art obfuscation based countermeasures are vulnerable to layout based reverse engineering attacks or Reset-and-scan attack where as the proposed methodology can withstand all such attacks. Hence, using the proposed methodology, the design can be made secure even in the presence of layout based reverse engineering attack, Reset-and-scan attack and scanSAT attack.

IV. CONCLUSION

We introduced scan camouflaging flipflop methodology to resist scan based attacks that are mainly employed to decode camouflaged combinational logic using Incremental SAT algorithms. The dummy port (DSI) which is added using dummy contacts inside the flipflop creates confusion on which is the real scan input port. This technique has an advantage over the state of the art techniques like Encrypt flipflop [11] and Scrambling [10] as it is not effected by reset-and-scan attack or layout based reverse engineering attacks. We validated the proposed methodology with IWLS-2005 benchmark circuits. From experimental results, it is concluded that the proposed technique has no impact on power and scan test time. There is a maximum of 2.2% impact on delay with 50% obfuscation. Furthermore, we also analysed the robustness of the proposed method when subjected to ScanSAT attack with and without scan compression. Our proposed methodology can secure the design from Incremental SAT-based attack and ScanSAT attack.

REFERENCES

[1] Leonardo R. Juracy, Matheus T. Moreira, Felipe A. Kuentzer, and Alexandre M. Amory, *A DfT Insertion Methodology to Scannable Q-Flop Elements*, IEEE transactions on very large scale integration (VLSI) systems, 2018.

[2] Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre, *New security threats against chips containing scan chain structures*, Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pages 110–110, 2011.

[3] Yier Jin, *Design-for-security vs. design-for-testability: A case study on dft chain in cryptographic circuits*, Proceedings of IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pages 19–24. IEEE, 2014.

[4] Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre,and Ingrid Verbauwhede, *Test versus security: past and present*, IEEE Transactions on Emerging topics in Computing, 2(1):50–62,2014.

[5] Duo Liu, Cunxi Yu, Xiangyu Zhang, and Daniel Holcomb, *Oracle guided incremental SAT solving to reverse engineer camouflaged logic circuits*, Proceedings of the 2016 Conference on Design, Automation Test in Europe, EDA Consortium,2016.

[6] Jeyavijayan Rajendran, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri, *Security analysis of integrated circuit camouflaging*, Proceedings of ACM SIGSAC conference on Computer & communications security, pages 709–720, 2013.

[7] Shweta Malik, Georg T Becker, Christof Paar, and Wayne P Burleson, *Development of a layout-level hardware obfuscation tool*, Proceedings of IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pages 204–209, 2015.

[8] C. Yu, X. Zhang, D. Liu, M. Ciesielski, and D. Holcomb, *Incremental sat-based reverse engineering of camouflaged logic circuits*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,36(10):1647–1659, 2017.

[9] Shuai Chen, Junlin Chen, Domenic Forte, Jia Di, Mark Tehranipoor, and Lei Wang, *Chip-level anti-reverse engineering using transformable interconnects*, Proceedings of IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), pages 109–114,2015.

[10] David Hely, Marie-Lise Flottes, Frederic Bancel, Bruno Rouzeyre, Nicolas Berard and Michel Renovell, *Scan design and secure chip*, Proceedings of IEEE International On-Line Testing Symposium (IOLTS), volume 4, pages 219–224, 2004.

[11] Rajit Karmakar, Santanu Chattopadhyay, and Rohit Kapur, *Encrypt Flip-Flop: A Novel Logic Encryption Technique For Sequential Circuits*, arXiv preprint arXiv:1801.04961, 2018.

[12] Lilas Alrahis, Muhammad Yasiny, Hani Saleh, Baker Mohammad, Mahmoud Al-Qutayri and Ozgur Sinanoglu, *ScanSAT: Unlocking Obfuscated Scan Chains*, Association for Computing Machinery, 2019.

[13] Mohamed El Massad, Siddharth Garg and Mahesh Tripunitara, *Reverse Engineering Camouaged Sequential Circuits Without Scan Access*, Computer-Aided Design (ICCAD),IEEE/ACM International Conference, 2017.

[14] J. P. Baukus, L. W. Chow, R. P. Cocchi, P. Ouyang, and B. J. Wang,"Camouflaging a standard cell based integrated circuit," US Patent no.8151235, 2012.

[15] J. P. Baukus, L.-W. Chow, J. W. M. Clark, and G. J. Harbison, "Conductive channel pseudo block process and circuit to inhibit reverse engineering," US Patent no. 8258583, 2012.

[16] Shahed E. Quadir, Junlin Chen, Domenic Forte, Navid Asadizanjani, Sina Shahbazmohamadi, Lei Wang, John Chandy, and Mark Tehranipoor. 2016. A Survey on Chip to System Reverse Engineering. J. Emerg. Technol. Comput. Syst. 13, 1, Article 6 (April 2016), 34 pages. DOI: https://doi.org/10.1145/2755563