ScanCamouflage: Obfuscating Scan Chains with Camouflaged Sequential and Logic Gates

Tarik Ibrahimpasic[1], Grace Li Zhang[3], Michaela Brunner[2], Georg Sigl[2,4], Bing Li[1], Ulf Schlichtmann[1]
[1]Chair of Electronic Design Automation, [2]Chair of Security in Information Technology, TU Munich, Germany
[3]Hardware for Artificial Intelligence Group, Technical University of Darmstadt, Germany
[4]Fraunhofer Institute for Applied and Integrated Security (AISEC), Garching b. Munich, Germany
{tarik.ibrahimpasic, michaela.brunner, sigl, b.li, ulf.schlichtmann}@tum.de, grace.zhang@tu-darmstadt.de

***Abstract*—Scan chain is a commonly used technique in testing integrated circuits as it provides observability and controllability of the internal states of circuits. However, its presence can make circuits vulnerable to attacks and potentially result in confidential internal data leakage. In this paper, we propose a novel technique for obfuscating scan chains using camouflaged flip-flops, which are designed with the same layout as the original flip-flops but have the actual functionality of a buffer. Furthermore, we employ camouflaged logic gates interconnected in special configurations to increase the difficulty of SAT attack. Experimental results demonstrate that circuits with only a small number of flip-flops can already be protected by the proposed technique while incurring only a minimal area overhead.**

***Index Terms*—scan chain obfuscation, gate camouflage**

I. Introduction

Reverse engineering of integrated circuits is a common attack that can result in significant risks, including intellectual property theft, counterfeiting, etc. Various techniques have been proposed to guard against reverse engineering, including logic locking [1], camouflaging [2] and insertion of wave-pipelining paths [3], [4]. Boolean satisfiability attacks (SAT attacks) [5] have proven to be effective at overcoming these techniques by utilizing the Boolean representation of a combinational circuit.

To attack a sequential circuit, access to the scan chain is usually assumed, making flip-flops in the circuit controllable and observable. Thus, the formulation of the SAT attack becomes similar to that of combinational circuits. Dynamic scan obfuscation [6] was proposed to protect the scan chain by inserting key-driven logic between scan flip-flops and updating the obfuscation key periodically. However, this technique requires the testing flow to be adapted, and moreover, it was already successfully deobfuscated by ScanSAT attack [7].

In this paper, we introduce a technique to obfuscate the scan chain by inserting camouflaged flip-flops with a buffer functionality. This is implemented by a new approach to modify the doping of the original flip-flop gate without changing its layout. Accordingly, SAT attacks relying on scan-chain access do not work anymore. Additionally, camouflaged logic gates are utilized to introduce fake cyclical paths, further complicating potential attacks. The testing procedure remains unchanged.

II. Scan Chain Obfuscation

A. Main Concept

To protect the scan chain, an obfuscation technique based on camouflaged flip-flops is proposed. Such components are designed with the same layout as the original flip-flops, but their functions are converted into buffers by doping modifications. While shifting in a test sequence, the camouflaged flip-flops forward the bits to the next real flip-flops in the chain instantly. In this way, the attacker, who is unaware of the locations of such gates, cannot control nor observe the desired flip-flops in the chain. This concept is illustrated in Fig. 1, where a scan chain with four flip-flops is depicted, one of which is camouflaged into a buffer. In a simple shift mode attack, the same scan-in sequence produces the same scan-out sequence for both cases when the camouflaged flip-flop is F2 and when it is F3. The testing functionality is unaffected since the generated test patterns can be applied and read out in the same manner.

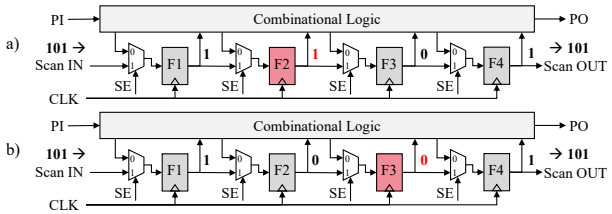

Fig. 1. Effect of a camouflaged flip-flop on the scan chain. a) Flip-flop F2 is camouflaged. b) Flip-flop F3 is camouflaged.

B. Gate Camouflage

The camouflaging method proposed in this paper alters the functionality of the original cells by doping modifications while not incurring additional fabrication masks. The method is shown in Fig. 2 using the example of a flip-flop DFFR_X1 gate from 45nm NanGate library [8]. By studying its structure, a clock stage, an active-low latch, an active-high latch, and an output stage can be identified. In the active-high latch part, a p-well and an n-well are interchanged under the poly gate of M18 and M19 transistors, effectively shorting them. The other two transistors on this path, M17 and M20, then form an inverter. Meanwhile, M22 and M23 transistors are disconnected by changing the dopants around the poly gate. The active-high latch is thus bypassed, and the flip-flop is modified into a latch that is transparent when the clock signal is low.

The active-low latch can be further converted into a buffer by changing the doping in the clock stage. The signal net_0, which is the inverted clock signal in the original gate, is connected to VDD by shorting the M1 transistor. To prevent the short-circuit between VDD and VSS, the M2 transistor is disconnected. Since the net_0 signal opens the active-low latch when it

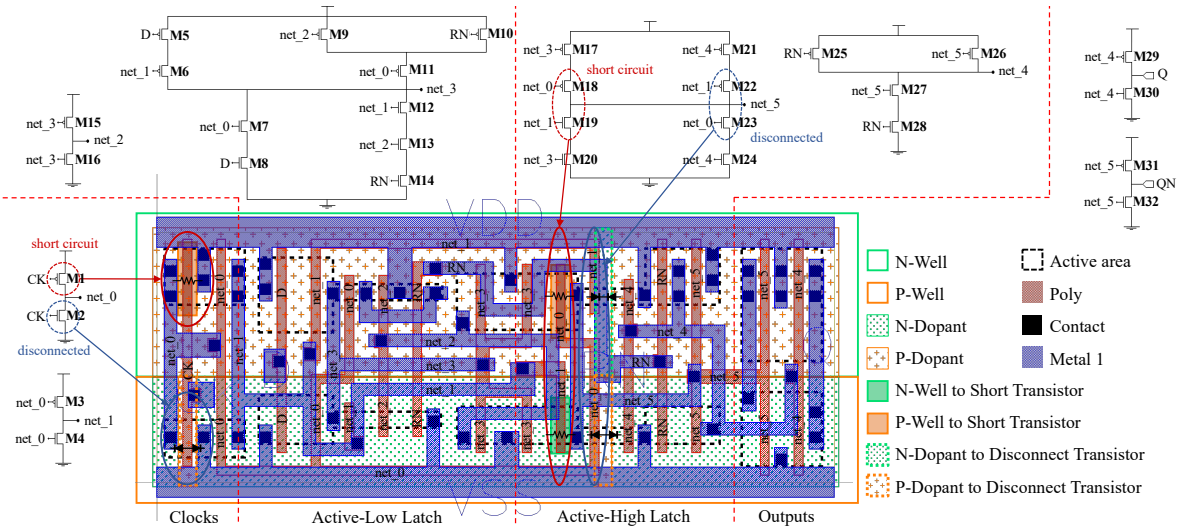

Fig. 2. Modified DFFR_X1 flip-flop, resulting in a buffer functionality (FF_B).

is high, the latch is always transparent, and the whole gate functions as a buffer, which is henceforth called an FF_B gate.

Other logic gates can be camouflaged similarly. For instance, a NAND gate can be modified into an inverter by shorting/disconnecting transistors that are controlled by one of its input pins. This effectively disconnects the input pin from the gate and makes the output of this gate not affected by it.

C. Insertion Strategy

Usually in regular designs, many flip-flops have combinational feedback paths. On the other hand, the inserted camouflaged flip-flops cannot have any combinational feedback paths, since that would presume the existence of combinational loops. By observing if a flip-flop has a feedback path, an attacker can easily recognize that the flip-flop is real, reducing the attack's scope. To hide the real flip-flops, FF_B gates are inserted in particular places in the design to minimize the number of self-looped flip-flops. Additionally, two-input NAND and NOR gates converted into inverters are utilized, with the disconnected input pin used to create cyclical paths. These camouflaged inverter gates are referred to as INV_C in the next section.

III. Experimental Results

Since all flip-flops are treated as potential FF_B gates during an attack, combinational loops are created if flip-flops have feedback paths. Hence, the open-source CycSAT attack [9] that can break loops in the Boolean formulation was used to locate the FF_B and INV_C gates. The attack was performed on a server with a 3.40 GHz Xeon E-2124G processor with 32 GB of RAM memory. The operating system was Linux.

The general performance of the obfuscation technique was analyzed using ISCAS89 benchmarks, and the results are shown in Fig 3. The number of inserted FF_B gates was a certain percentage of the total number of flip-flops in the circuit. Additionally, a certain percentage of inverters were selected and replaced with INV_C gates, half of them having a layout of a two-input NAND gate and half of a two-input NOR gate. All flip-flops were interconnected in the scan chain. Since different scan chain orders could lead to different attack results, ten

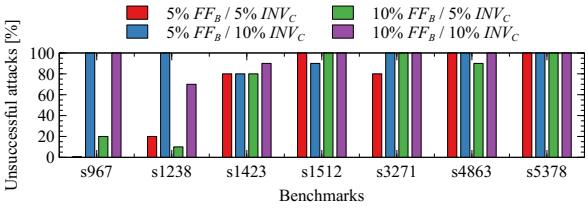

Fig. 3. Percentage of CycSAT attacks reaching timeout.

different scan chain orders were generated randomly for each benchmark to obtain a rough estimation. The timeout value was set to 1 hour. As shown from Fig 3, the CycSAT attack reached a timeout in most cases by running into an infinite loop. The effect was more pronounced in bigger benchmarks and for a higher percentage of INV_C gates inserted.

IV. Conclusion

We have proposed a novel approach for scan chain obfuscation by using camouflaged sequential and logic gates. We demonstrated that a high level of scan chain obfuscation can be achieved with a minimal area overhead while not affecting the original testing functionality.

Acknowledgment

This work is funded by the German Federal Ministry of Education and Research through Project VE-FIDES under Grant 16ME0257.

References

[1] J. A. Roy, F. Koushanfar, and I. L. Markov, "EPIC: Ending Piracy of Integrated Circuits," in *2008 Design, Automation and Test in Europe*, pp. 1069–1074, 2008.

[2] B. Shakya, H. Shen, M. Tehranipoor, and D. Forte, "Covert Gates: Protecting Integrated Circuits with Undetectable Camouflaging," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 86–118, 2019.

[3] G. L. Zhang, B. Li, B. Yu, D. Z. Pan, and U. Schlichtmann, "TimingCamouflage: Improving Circuit Security Against Counterfeiting by Unconventional Timing," in *2018 Design, Automation Test in Europe*, pp. 91–96, 2018.

[4] G. L. Zhang, B. Li, M. Li, B. Yu, D. Z. Pan, M. Brunner, G. Sigl, and U. Schlichtmann, "TimingCamouflage+: Netlist Security Enhancement With Unconventional Timing," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 12, pp. 4482–4495, 2020.

[5] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the Security of Logic Encryption Algorithms," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 137–143, 2015.

[6] X. Wang, D. Zhang, M. He, D. Su, and M. Tehranipoor, "Secure Scan and Test Using Obfuscation Throughout Supply Chain," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 9, pp. 1867–1880, 2018.

[7] L. Alrahis, M. Yasin, N. Limaye, H. Saleh, B. Mohammad, M. Al-Qutayri, and O. Sinanoglu, "ScanSAT: Unlocking Static and Dynamic Scan Obfuscation," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1867–1882, 2021.

[8] "15nm Open-Cell library and 45nm freePDK." https://si2.org/open-cell-library/.

[9] H. Zhou, R. Jiang, and S. Kong, "CycSAT: SAT-based Attack on Cyclic Logic Encryptions," in *2017 IEEE/ACM International Conference on Computer-Aided Design*, pp. 49–56, 2017.