

# Lifetime Reliability Trojan based on Exploring Malicious Aging

Tien-Hung Tseng and Kai-Chiang Wu

Department of Computer Science

National Chiao Tung University, Hsinchu, Taiwan

E-mail: {eric830303.cs05g@g2.nctu.edu.tw and kcw@cs.nctu.edu.tw}

**Abstract**—Due to escalating complexity of hardware design and manufacturing, not only are integrated circuits (ICs) designed and fabricated in multiple nations, but also software tools may be supplied worldwide. It makes hardware security become more subject to various kinds of tampering in the supply chain. Hardware Trojan horses (HTHs) can be implanted to facilitate the leakage of confidential information or cause the failure of a system. Reliability Trojan is one of the main categories of HTH attacks because its behavior is progressive and is thus not trivial to be detected, or not considered malicious. In this work, we propose to insert reliability Trojan into a circuit which can finely control the circuit lifetime as specified by attackers (or even designers), based on manipulating BTI-induced aging behavior in a statistical manner. Experimental results show that, given a specified lifetime target and under the influence of process variations, the circuit is highly likely to fail within a desired lifetime interval. Instead, in a typical design considering pessimistic corners, the resulting lifetime is usually far longer than the target.

## I. INTRODUCTION

Due to escalating complexity of hardware design and manufacturing [1], integrated circuits (ICs) are usually designed and fabricated in multiple locations worldwide. Moreover, some design tools are also supplied from different units. With the utilization of third-party IP components and off-shore IC manufacturing, the overall cost and time-to-market are significantly reduced. However, hardware security becomes more subject to various kinds of tampering in the supply chain [2][3]. Typically, a hardware system does no more than its requirements. Doing more than required, hardware Trojan horses (HTHs) can be implanted to facilitate the leakage of confidential information or cause the failure of a system [4]-[5]. Outsourcing (e.g., third-party IP components, design tools and off-shore IC manufacturing) makes malicious HTH attacks possible. In order to introduce the motivation of deploying HTH attacks, here we make some scenario from various aspects, i.e., attackers. Manufacturers: Given a design house A with its competitor B, in order to interfere B's commercial development, A paid B's ICs manufacturer M such that M tampered B's layout, making B's product(s) malfunction earlier than expected. Design-tool suppliers: Given a country C with its imaginary enemy D, and we assume that D's design houses utilize at least one design tool supplied from C's software corporation S. For the purpose of obstructing D's high-tech military weapon development, C forced S to embed malicious mechanisms in its software merchandise. Therefore,

no matter what kinds of military equipment D produces, they are stealthily put HTH in the inner ICs. After the insertion of HTHs, it is difficult to prove their existence since they are pervasive and inappreciable. In this sense, the proposed research provides new primitives for aforementioned hardware security threats, by exploring the feasibility of different HTH attacks and associated detection/prevention countermeasures. Reliability Trojan is one of the main categories of HTH attacks because its behavior is progressive and is thus not trivial to be detected, or not considered malicious. Time-dependent dielectric breakdown (TDDB), bias temperature instability (BTI), and electromigration (EM) are some of the critical failure mechanisms affecting lifetime reliability. With the continuous shrinking of transistor and interconnect dimensions, the rate of such progressive wear-out failures is getting higher. In addition, due to the increasing transistor density without proportional downscaling of supply voltage, the power density and thus the operating temperature will rise significantly, which further accelerates the failure mechanisms because they are all exponentially dependent on temperature. In this work, we propose to insert reliability Trojan into a circuit which can finely controls the circuit lifetime as specified by attackers (or even designers), based on manipulating BTI-induced aging behavior in a statistical manner.

## II. RELATED WORK

Studies about reliability Trojan have been proposed since last few years. [6] details BTI and HCI effects which induce aging failures, and accelerates the effects by aggravating the most influential parameters of BTI and HCI. [7] proposes a few Trojan designs which accelerate EM, BTI and TDDB effects by stressing/modifying specific interconnects and gates. Some studies also try to control the lifetime of a circuit by counters or timers. In [8], authors present a Trojan which controls lifetime by analog mechanism. It siphons charge from target wire and stores to a capacitor until voltage on the capacitor rises above the threshold and sets its output flip-flop to a desired value. [9] presents an unmodified Trojan by analyzing the netlist of a circuit to identify its critical paths; then they generate patterns/instructions for stressing those paths. These patterns can be fed by external programs or embedded devices to accelerate the aging and decrease the circuit performance and lifetime. [8] [9] focus on the logic blocks which highly depend on users' operational modes.

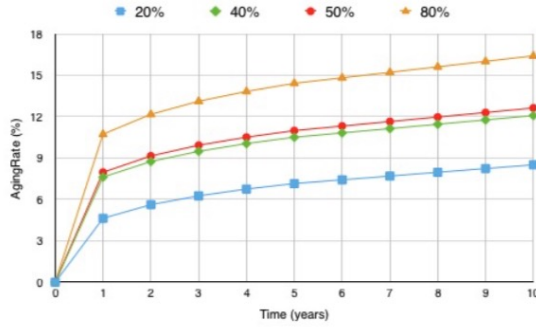


Figure 1. aging rates of buffers with different clock duty cycles

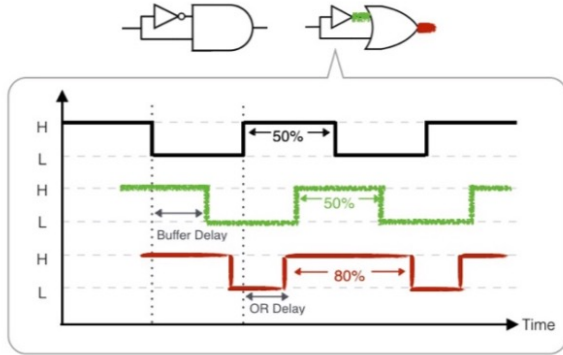


Figure 2. Construction of DCC and duty-cycle transformation

However, [6] does not estimate circuit lifetime in detail and [7] has relatively high cost based on using counters to control lifetime. To predict circuit lifetime with Trojans, [10] uses mathematical modeling to estimate circuit reliability, but it only tries on tiny circuit C17 and does not consider aging. In addition, [11] proposes an idea using aging effects to induce a circuit into its redundant states (i.e., operational modes) and thereafter execute malicious function. This paper proposes a method of hardware Trojan insertion to control the lifetime of a circuit based on manipulating the rate of circuit aging. We consider (i) the aging of both clock trees and combinational logical paths, and (ii) the correlation of aging rates between critical paths. These considerations ensure the effect of our proposed Trojan to be manifested on time under all possible workloads due to various users' operational conditions. More clearly, we present a methodology that deploys duty-cycle converters (DCCs) into a clock tree to accelerate the aging of predesignated clock buffers/inverters associated with critical paths. Those paths will fail around the time we set regardless of operational conditions.

### III. MOTIVATING EXAMPLE

#### A. Duty-Cycle Converter (DCC)

Duty cycle is the percentage of one period in which a signal is high (i.e., logic 1). We have known that the aging of logic gates highly depends on the stress time [8]. For a clock buffer

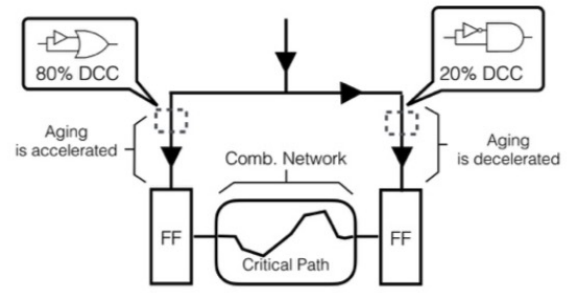


Figure 3. Example of DCC insertion

on the clock tree, its stress time is proportional to the clock duty cycle. Therefore, by adjusting the clock duty cycle, we can manipulate the aging of clock buffers and then control the effective degradation of logic paths. 1 shows the aging rates of clock buffers with different clock duty cycles. The unit we use to change the clock duty cycle is duty-cycle converter (DCC). A DCC includes an inverter/buffer and an AND/OR gate. It can convert the duty cycle of a clock signal to a smaller/larger one. 2 shows a DCC and the conversion of the clock duty cycle from 50% to 80%. It separates the source clock wave (black line) to a delayed wave (green line, may be inverted) and original wave. Then, those two waves are combined with the OR gate to obtain a new clock wave (red line) of 80% duty cycle.

#### B. DCCs against a Critical Path

Once we insert a DCC into the clock tree, the downstream sub-tree of the DCC insertion point will receive a clock signal whose duty cycle is no longer 50%. Consider the circuit in 3: we insert an 80% DCC on the left clock path to accelerate its aging and a 20% DCC on the right clock path to decelerate its aging. Over several years, the left clock latency will gain greater than the right one does. Therefore, setup-time violations are likely to occur on this critical path.

### REFERENCES

- [1] L. Wilson, "International technology roadmap for semiconductors (itrs)," *Semiconductor Industry Association*, 2013.
- [2] M. Tehranipoor *et al.*, "Trustworthy hardware: Trojan detection and design-for-trust challenges," *Computer*, vol. 44, no. 7, pp. 66–74, 2011.
- [3] R. Karri *et al.*, "Trustworthy hardware: Identifying and classifying hardware trojans," *Computer*, vol. 43, no. 10, pp. 39–46, 2010.
- [4] S. Adek, "The hunt for the kill switch," *IEEE Spectrum*, vol. 45, no. 5, pp. 34–39, 2008.
- [5] S. Bhunia *et al.*, "Hardware trojan attacks: Threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.
- [6] Y. Shiyonovskii *et al.*, "Process reliability based trojans through nbt and hci effects," in *Adaptive Hardware and Systems (AHS), 2010 NASA/ESA Conference on*, IEEE, 2010, pp. 215–222.
- [7] A. Sreedhar, S. Kundu, and I. Koren, "On reliability trojan injection and detection," *Journal of Low Power Electronics*, vol. 8, no. 5, pp. 674–683, 2012.
- [8] K. Yang *et al.*, "A2: Analog malicious hardware," in *Security and Privacy (SP), 2016 IEEE Symposium on*, IEEE, 2016, pp. 18–37.
- [9] N. Karimi *et al.*, "Magic: Malicious aging in circuits/cores," *ACM Transactions on Architecture and Code Optimization (TACO)*, vol. 12, no. 1, p. 5, 2015.

- [10] S. Burman *et al.*, “Effect of malicious hardware logic on circuit reliability,” in *Progress in VLSI Design and Test*, Springer, 2012, pp. 190–197.
- [11] S. Wei and M. Potkonjak, “The undetectable and unprovable hardware trojan horse,” in *Proceedings of the 50th Annual Design Automation Conference*, ACM, 2013, p. 144.