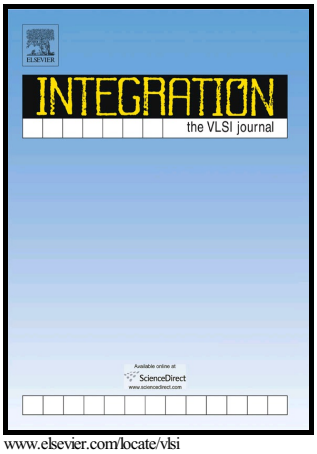

www.elsevier.com/locate/vlsi

Self-triggering Hardware Trojan: Due to NBTI Related Aging in 3-D ICs

Siraj Fulum Mossa, Syed Rafay Hasan, Omar Elkeelany

PII: S0167-9260(16)30223-1
DOI: http://dx.doi.org/10.1016/j.vlsi.2016.12.013
Reference: VLSI1289

To appear in: *Integration, the VLSI Journal*

Received date: 17 June 2016
Revised date: 1 November 2016
Accepted date: 28 December 2016

Cite this article as: Siraj Fulum Mossa, Syed Rafay Hasan and Omar Elkeelany Self-triggering Hardware Trojan: Due to NBTI Related Aging in 3-D ICs *Integration, the VLSI Journal,* http://dx.doi.org/10.1016/j.vlsi.2016.12.013

Self-triggering Hardware Trojan: Due to NBTI Related Aging in 3-D ICs

Siraj Fulum Mossa*, Syed Rafay Hasan, Omar Elkeelany
Department of Electrical and Computer Engineering, Tennessee Tech University, Cookeville, TN 35805, USA
Email: *siratmit@gmail.com

Abstract—

3-D ICs provide more transistor density and higher performance at smaller area compared to traditional 2-D ICs. However, elevated temperatures and longer heat dissipation paths in 3-D IC can lead to non-ideal delay variations. Higher temperatures lead to negative bias temperature instability (NBTI), and consequently shifts threshold voltage (V_{th}), which leads to current degradation and delay increment. These variations can be exploited by hardware intruder and introduce malicious circuit components causing malfunctioning in 3-D ICs. This paper takes the threat model in which the attacker has access to the hard-intellectual property (IP) development, and defender is at the foundry. This paper demonstrates that a hardware intruder can leverage the exacerbated NBTI effect to trigger the Trojan payload. Consequently, such Trojans does not require a conventional triggering circuit; hence we named it as self-triggered. The proposed hardware Trojan is very difficult to detect and can scape various countermeasures at testing phase due to 'non-existing triggering signal'. The point of attack for the proposed Trojan is the body of the semiconductor device, for example, the body of PMOS device. When the Trojan gets activated it shorts the body and source of the PMOS to ground leading the device without power supply. We discussed the stealthy nature of our proposed Trojan against the existing countermeasures and also provided a discussion on a novel avenue of detecting such kinds of hardware Trojans.

Keywords: 3-D IC, hardware Trojan, NBTI

I. Introduction

Due to stacking of active Silicon layers vertically in 3-D IC the average distance from the heat sinks to the top tiers of 3-D ICs is higher than the bottom layers, where the heat sink resides. Temperature increases as we go farther away from the heat sink. Hence, temperature across the tiers varies considerably. This non-uniform dynamic thermal variation may lead to non-uniform delay variations across the chip [1-5]. As shown in Fig. 1, the temperature distribution varies a lot among different layers. More tiers lead to more accumulative thermal resistance, which leads to higher temperature.

The 2-D dies are stacked, bonded and electrically interconnected vertically Through Silicon Via (TSV) in 3-D IC. For miniaturization purposes these dies are usually made as thin as 20 µm [1]. Hence, each die consists of less Silicon (relatively good heat conductor) and more oxide and molding compound (relatively poorer heat conductor). This complicates the heat conduction paths, and can deteriorate the worst-case heat dissipation path. Consequently, a given power density may produce a wider variation in temperature in 3-D IC. Also, stacking multiple dies into the same footprint formerly occupied by 2-D IC, leads to higher temperature for the same amount of power dissipation, [1]. Hence, temperature variations are likely to increase in 3-D ICs than 2-D ICs.

Because of the proximity of active Silicon layers and longer heat dissipating paths from the heat sink, the top layer of 3-D IC faces a critical challenge of dissipating higher thermal energies. Kiran et al. [5] reports the estimation of temperatures for the implementation of the same circuit in planar 2-D IC, 2-die (tiers) 3-D IC and 4-die (tiers) 3-D ICs. Compared to the planar IC, the 2-die and 4-die 3-D IC implementations experience increment in the maximum temperature by 17 ^{0}K and 33 ^{0}K, respectively. Subsequently, the issue of inefficient thermal dissipation in 3-D ICs exacerbates the effect of negative bias temperature instability (NBTI), which can lead to faster aging of ICs. NBTI happens whenever a PMOS transistor is negatively biased (i.e. when the gate voltage is at GND and the source voltage is at VDD) at elevated temperatures. This results in increase in the absolute threshold voltage, degradation of the mobility carriers, drain current, and trans-conductance of p-channel MOSFETs [6-10]. This causes delay to increase, and if not properly provisioned for, can result in timing violations.

It is known to researchers that the dominant aging effect for semiconductor devices is induced by NBTI. For example, threshold voltage degrades by 50mV in 7 to 10 years after the manufacturing of ICs, due to aging caused by NBTI, [8]. This threshold voltage degradation may lead to 20% speed degradation. Also, as technology scales, transistor aging for nano-scale devices poses a key challenge for designers to find countermeasures that can effectively mitigate the degradation and threshold voltage shifting. Balaji et al. [9] reports a strong correlation between NBTI-induced time delays with threshold voltage shift.