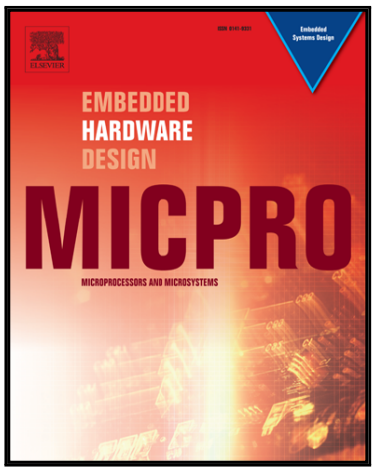

Behavioral-Level Hardware Trust: Analysis and Enhancement

Najmeh Farajipour Ghohroud , Shaahin Hessabi

PII: S0141-9331(17)30246-6
DOI: 10.1016/j.micpro.2018.02.002
Reference: MICPRO 2656

To appear in: *Microprocessors and Microsystems*

Received date: 17 May 2017
Revised date: 18 November 2017
Accepted date: 9 February 2018

Please cite this article as: Najmeh Farajipour Ghohroud , Shaahin Hessabi , Behavioral-Level Hardware Trust: Analysis and Enhancement , *Microprocessors and Microsystems* (2018), doi: 10.1016/j.micpro.2018.02.002

Behavioral-Level Hardware Trust: Analysis and Enhancement

Najmeh Farajipour Ghohroud[*1], Shaahin Hessabi [1]
[1] Department of Computer Engineering, Sharif University of Technology, Tehran, IRAN
[*] farajipour@ce.sharif.edu

Abstract: Hardware IPs are mostly presented in Register Transfer Level (RTL) description. Although considerable attention has been paid to hardware Trojan detection and design-for-trust at gate level and lower levels, so far there have been few methods at RT Level and behavioral RTL. We propose an approach to analyze circuit susceptibility to Trojan at the behavioral level, based on controllability analysis. We propose three design-for-trust methods, which reduce circuit vulnerability to hardware Trojans by increasing the probability of Trojan detection. We use side-channel Trojan detection method based on power consumption to evaluate Trojan detection probability. Our proposed methods can improve Trojan detection probability by up to 5 times, with negligible hardware overhead.

Keywords: Hardware Trojan, Trojan detection, Behavioral level, Controllability

1. INTRODUCTION

Most hardware manufacturers outsource fabrication of their integrated circuits (ICs) to third party foundries in order to reduce the cost of silicon chip fabrication [1]. This increases the vulnerability to malicious activities. Third party foundries may modify the circuit's design or its physical parameters. These modifications are known as Hardware Trojan Horses (HTH). An adversary can insert a Trojan in the design to disable and/or destroy a system. Moreover, the Trojan may leak information to the adversary.

HTHs must be triggered by some internal or external events or a sequence of such events, to become operative. A smart adversary will try to hide such modification of IC's functional behavior in a way to make it very difficult to detect with conventional post–manufacturing test [2]. Therefore, the adversary would ensure that such modification is triggered under very rare conditions, which are unlikely to occur during test, but can arise during long period of field operation [3].

Hardware Trojans sizes measured in proportion with the size of the circuit are very small, and they have almost negligible effect on a circuit's parameters. Also, hardware Trojans are rarely fully activated, because their trigger inputs are most likely connected to nets with low controllability and/or observability [4], [5]. Therefore, detection of their malicious activities is very difficult. Several methods have been proposed to avoid Trojan insertion, or to facilitate its detection. These methods are classified as design-for-trust methods. To improve Trojan detection effectiveness, some techniques have been suggested to embed monitoring systems into the circuits to monitor circuit behavior and record any abnormality in circuit performance or power consumption [6], [7], [8], [9], [10], [11]. Several methods, which are proposed in the field of design-for-hardware-trust, have aimed to show Trojan effect on circuit behavior during authentication [12], [13], [14]. Likewise, several side-channel-based methods have been proposed to magnify the Trojan impact in the presence of process variations in a circuit [15], [16], [17], [18].

N. Farajipour Ghohroud, and S. Hessabi are with the Department of Computer Engineering, Sharif University of Technology, Tehran, IRAN.
(e-mail: farajipour@ce.sharif.edu, hessabi@sharif.edu).