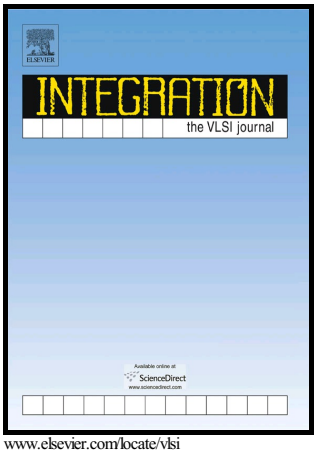
Author's Accepted Manuscript



www.elsevier.com/locate/vlsi

A hardened network-on-chip design using Runtime hardware trojan mitigation methods

Jonathan Frey, Qiaoyan Yu

PII: S0167-9260(16)30031-1
DOI: http://dx.doi.org/10.1016/j.vlsi.2016.06.008
Reference: VLSI1225

To appear in: *Integration, the VLSI Journal*

Received date: 12 March 2016
Revised date: 13 June 2016
Accepted date: 27 June 2016

Cite this article as: Jonathan Frey and Qiaoyan Yu, A hardened network-on-chip design using Runtime hardware trojan mitigation methods, *Integration, the VLSI Journal,* http://dx.doi.org/10.1016/j.vlsi.2016.06.008

A Hardened Network-on-Chip Design using Runtime Hardware Trojan Mitigation Methods

Jonathan Frey, Qiaoyan Yu

University of New Hampshire, Durham, NH 03824 USA.

jpg73@wildcats.unh.edu

qiaoyan.yu@unh.edu

Abstract

Due to the globalized semiconductor business model, malicious hardware modifications, known as hardware Trojans (HTs), have risen up as a big concern for chip security. HT detection and mitigation methods for general integrated circuits have been investigated in the past decade. However, the majority of the existing efforts are not customized for HTs in Networks-on-Chip (NoCs). To complement the firmware and software level methods for rogue NoCs detection, we propose countermeasures to harden the NoC hardware design against tampering. More specifically, we propose a collaborative dynamic permutation and flit integrity check method to mitigate the potential inside-router HTs inserted by the disloyal member in the NoC design house or the 3rd-party system integration company. Our method improves the number of received packets by up to 70.1% over the other methods if the HT controls the NoC packet destination address. The average link availability of our method is 43.7% higher than that of the exiting methods. Our method increases the effective average latency by up to 63.4%, 68.2%, and 98.9% for the single HT in the destination, header, and tail fields, respectively, over the existing methods.

Index Terms—Network-on-chip (NoC), hardware Trojan, hardware security, bandwidth depletion, deadlock, livelock, denial-of-service attack, latency, throughput.

INTRODUCTION

OUTSOURCED fabrication, assembly and testing, have resulted in chip designs facing a new challenge—threats on hardware security [1-4]. Among various hardware threats, hardware Trojans (HTs) are a well-known one; which are malicious hardware modifications on the original chip. An HT is composed of trigger circuit and payload circuit. The trigger circuit is used to examine the arrival of the trigger condition that the attacker specifies in the Trojan insertion stage. The Trojan payload circuit could cause a denial-of-service (DoS) problem, alter a chip's normal operations, or provide the adversary with the privilege to access a confidential memory space [5-7]. The Semiconductor Research Corporation (SRC)

This manuscript was submitted on March 11st, 2016, and revised on June 13rd, 2016.

.