1. Detecting Hardware Trojans using On-chip Sensors in an ASIC Design

Accession number: 15534903
Authors: Kelly, S. (1); Xuehui Zhang (1); Tehranipoor, M. (1); Ferraiuolo, A. (2)
Author affiliation: (1) Dept. of Electr. & Comput. Eng., Univ. of Connecticut, Storrs, CT, United States; (2) Dept. of Electr. & Comput. Eng., Cornell Univ., Ithaca, NY, United States
Source title: Journal of Electronic Testing. Theory and Applications
Abbreviated source title: J. Electron. Test., Theory Appl. (USA)
Volume: 31
Issue: 1
Publication date: Feb. 2015
Pages: 11-26
Language: English
ISSN: 0923-8174
CODEN: JTTAER
Document type: Journal article (JA)
Publisher: Springer
Country of publication: USA
Material Identity Number: ET30-2015-001
Abstract: The modern integrated circuit (IC) manufacturing process has exposed the fabless semiconductor industry to hardware Trojans that threaten circuits bound for critical applications. This paper investigates an on-chip sensor's effectiveness for Trojan detection in an application specific integrated circuit (ASIC) and proposes new techniques to improve the sensor's sensitivity to Trojan switching activity. The sensors serve as power supply monitors by detecting fluctuations in their characteristic frequencies due to malicious inclusions (i.e. hardware Trojans) in the circuit under authentication. Our proposed on-chip structure was implemented and fabricated on an ASIC test chip using IBM 90nm technology with controlled hardware Trojans. This work analyzes the impact of both sequential and combinational Trojans with varied partial activity, area, and location on the proposed on-chip structure and demonstrates that stealthy Trojans can be effectively detected with this technique, even when obfuscated by circuit switching activity and process and environmental variations.
Number of references: 27
Inspec controlled terms: application specific integrated circuits - integrated circuit design - integrated circuit testing
Uncontrolled terms: hardware Trojan detection - on-chip sensor effectiveness - ASIC design - integrated circuit manufacturing process - IC manufacturing process - fabless semiconductor industry - application specific integrated circuit - sensor sensitivity - Trojan switching activity - ASIC test chip - IBM technology - combinational Trojans - sequential Trojans - partial activity - circuit switching activity - size 90 nm
Inspec classification codes: B1280 Mixed analogue-digital circuits - B2570A Semiconductor integrated circuit design, layout, modelling and testing - B1205 Analogue circuit design, modelling and testing
Numerical data indexing: size 9.0E-08 m
Treatment: Practical (PRA); Theoretical or Mathematical (THR)
Discipline: Electrical/Electronic engineering (B)
DOI: 10.1007/s10836-015-5504-x
IPC Code: G01R31/28
Database: Inspec

Data Provider: Engineering Village