1. Side-channel analysis-based detection approach of hardware Trojans

Accession number: 20123515381792
Authors: Wang, Li-Wei (1, 2); Luo, Hong-Wei (2); Yao, Ruo-He (1)
Author affiliation: (1) School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510640, Guangdong, China; (2) Science and Technology on Reliability Physics and Application of Electronic Component Laboratory, The Fifth Electronics Research Institute of the Ministry of Industry and Information Technology, Guangzhou 510610, Guangdong, China
Corresponding author: Wang, L.-W.(wanglw@ceprei.com)
Source title: Huanan Ligong Daxue Xuebao/Journal of South China University of Technology (Natural Science)
Abbreviated source title: Huanan Ligong Daxue Xuebao
Volume: 40
Issue: 6
Issue date: June 2012
Publication year: 2012
Pages: 6-10
Language: Chinese
ISSN: 1000565X
CODEN: HLDKEZ
Document type: Journal article (JA)
Publisher: South China University of Technology, Guangzhou, 510640, China
Abstract: During the fabrication of integrated circuit (IC) chips in untrusted foundries, malicious circuits may be inserted as hardware Trojans, which results in a significant risk of trustworthiness and reliability degradation of the chips. As such Trojan circuits are difficult to detect using conventional strategies, a nondestructive side-channel analysis-based detection approach is proposed, which employs the algorithm of singular value decomposition to analyze and statistically process the transient power of IC chips. Validation results of the approach on FPGA chips show that, even in the presence of big noise and process variation, the proposed approach is effective in detecting the hardware Trojans that are 2 orders of magnitude smaller than the original circuit.
Number of references: 13
Main heading: Hardware
Controlled terms: Degradation - Field programmable gate arrays (FPGA) - Singular value decomposition
Uncontrolled terms: Detection approach - FPGA chips - IC chips - Integrated circuit chips - Non destructive - Orders of magnitude - Process Variation - Reliability degradation - Side-channel - Side-channel analysis - Trojans - Validation results
Classification code: 605 Small Tools and Hardware - 721.3 Computer Circuits - 802.2 Chemical Reactions - 921 Mathematics
DOI: 10.3969/j.issn.1000-565X.2012.06.002
Database: Compendex

Data Provider: Engineering Village