1. The problem of hardware Trojans detection in system-on-chip

Accession number: 10588533
Authors: Adamov, A. (1); Saprykin, A. (1); Melnik, D. (1); Lukashenko, O. (1)
Author affiliation: (1) DAD Dept., Kharkov Nat. Univ. of Radio Electron., Kharkov, Ukraine
Source: 2009 10th International Conference. The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM 2009)
Publication date: 2009
Pages: 178-9
Language: English
ISBN-13: 978-1-4244-5387-0
Document type: Conference article (CA)
Conference name: 2009 10th International Conference. The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM 2009)
Conference date: 24-28 Feb. 2009
Conference location: Lviv-Polyana, Ukraine
Publisher: IEEE
Place of publication: Piscataway, NJ, USA
Material Identity Number: YXA9-1900-695
Abstract: This paper describes a new threat to the security of integrated circuits (ICs) called Hardware Trojans. Such alterations can be embedded in safety critical, security and military systems, such as weapon control systems, battlefield communication systems, information collection and decision making systems, satellite electronics, banking systems, cryptosystems, etc. The reason is the current trend of IC fabrication migration to low-cost foundries, where additional malicious circuits can be inserted by adversary that could result in functional changes and the whole system failure. The goal of the paper is to describe security problem in IC manufacturing, analyze the existed methods with their bottlenecks for effective Trojan detection in large ICs, such as system-on-chips (SoCs).
Number of references: 4
Inspec controlled terms: integrated circuit testing - security of data - system-on-chip
Uncontrolled terms: hardware Trojans detection - system-on-chip - integrated circuits security - safety critical - military systems - IC fabrication migration
Inspec classification codes: B1265F Microprocessors and microcomputers - B1265A Digital circuit design, modelling and testing - C5130 Microprocessor chips - C6130S Data security
Treatment: Practical (PRA)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
IPC Code: G01R31/28 - G06F15/76 - G06F21/00
Database: Inspec

Data Provider: Engineering Village