1. Hardware Enlightening: No Where to Hide Your Hardware Trojans!

Accession number: 16398233
Authors: Samimi, M.S. (1); Aerabi, E. (1); Kazemi, Z. (1); Fazeli, M. (1); Patooghy, A. (1)
Author affiliation: (1) Comput. Eng. Dept., Iran Univ. of Sci. & Technol., Tehran, Iran
Source: 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)
Publication date: 2016
Pages: 251-6
Language: English
ISBN-13: 978-1-5090-1507-8
Document type: Conference article (CA)
Conference name: 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)
Conference date: 4-6 July 2016
Conference location: Sant Feliu de Guixols, Spain
Sponsor: IEEE Council on Electron. Design Autom.
Publisher: IEEE
Place of publication: Piscataway, NJ, USA
Material Identity Number: YXB6-1902-553
Abstract: IC design and manufacturing chains show steadily growing complexity which provides different third party roles in between. Reprobate parties can take the opportunity to steal a client's IP or insert their malicious circuits-Hardware Trojans-in the original client's design and trigger them in case of need. Trojans are usually inserted in the most hidden internal signals with the lowest activity which increase their chance for not being activated and revealed by clients or end-users. In this paper we propose a method to reduce the number of signals with low activity and hence the chance of inserting hidden trojans. This method is based on an enhanced Logic Encryption approach and uses a 128-bit key. Encryption can also secure the design against IP piracy. Simulation results show that the proposed method can eliminate 83.17% of low activity signals in the circuit.
Number of references: 17
Inspec controlled terms: computer crime - cryptography - invasive software - logic gates
Uncontrolled terms: IC manufacturing chains - IC design chains - malicious circuits - hidden internal signals - hidden Trojans - enhanced logic encryption - client IP piracy - low activity signals - hardware trojans - word length 128 bit
Inspec classification codes: B1265B Logic circuits - C5480 Security aspects of hardware - C5110 Logic elements - C6130S Data security
Numerical data indexing: word length 1.28E+02 bit
Treatment: Practical (PRA)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
DOI: 10.1109/IOLTS.2016.7604712
IPC Code: G06F21/00 - H03K19/00
Database: Inspec

Data Provider: Engineering Village