1. Hardware Trojans detection based on projection pursuit

Accession number: 14007014
Authors: Zhang Peng (1); Wang Xin-cheng (1); Zhou Qing (1)
Author affiliation: (1) Sci. & Technol. on Inf. Assurance Lab., Beijing, China
Source title: Journal on Communications
Abbreviated source title: J. Commun. (China)
Volume: 34
Issue: 4
Publication date: April 2013
Pages: 122-6, 137
Language: Chinese
ISSN: 1000-436X
Document type: Journal article (JA)
Publisher: Editorial Board of the Journal of Communications
Country of publication: China
Material Identity Number: GC79-2013-006
Abstract: A novel hardware Trojans detection technique using the side channel signals of chips was proposed. Based on the projection pursuit with absolute information divergence index, this technique could find out the data structure enables reflect high dimension special rules without obvious information loss, so as to attain the goal of feature abstraction and identification on side channel signals of IC chips. The detection experiment against an exemplary AES-128 hardware Trojan circuit showed that the technique could distinguish the difference of side channel signal's feature between the genuine chip and tested chip, and consequently could detect the existence of the hardware Trojan.
Number of references: 11
Inspec controlled terms: cryptography - data analysis - data structures - invasive software - principal component analysis
Uncontrolled terms: exploratory data analysis - EDA - CDA - PCA - confirmatory data analysis - principal component analysis - tested chip - genuine chip - exemplary AES-128 hardware Trojan circuit - IC chips - feature identification - feature abstraction - data structure - absolute information divergence index - side channel signals - projection pursuit - novel hardware Trojans detection technique
Inspec classification codes: B6120D Cryptography - B0240Z Other topics in statistics - C6130S Data security - C1140Z Other topics in statistics
Treatment: Practical (PRA)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
DOI: 10.3969/j.issn.1000-436x.2013.04.014
IPC Code: G06F21/00 - H04L9/00
Database: Inspec
Copyright 2014, The Institution of Engineering and Technology
Data Provider: Engineering Village