1. A chip architecture for compressive sensing based detection of IC trojans

Accession number: 20131316150928

Authors: Tsai, Yi-Min (1); Huang, Keng-Yen (1); Kung, H.T. (2); Vlah, Dario (2); Gwon, Youngjune L. (2); Chen, Liang-Gee (1)
Author affiliation: (1) Graduate Institute of Electronics Engineering, National Taiwan University, Taiwan; (2) School of Engineering and Applied Sciences, Harvard University, United States
Corresponding author: Tsai, Y.-M.(ymtsai@video.ee.ntu.edu.tw)

Source title: IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation
Abbreviated source title: IEEE Workshop Signal. Process. Syst. SiPS Des. Implement.
Monograph title: Proceedings - 2012 IEEE Workshop on Signal Processing Systems, SiPS 2012
Issue date: 2012
Publication year: 2012
Pages: 61-66
Article number: 6363184
Language: English
ISSN: 15206130
ISBN-13: 9780769548562
Document type: Conference article (CA)
Conference name: 2012 IEEE Workshop on Signal Processing Systems, SiPS 2012
Conference date: October 17, 2012 - October 19, 2012
Conference location: Quebec City, QC, Canada
Conference code: 95856
Sponsor: IEEE Signal Processing Society; IEEE Circuits and Systems Society (CAS)
Publisher: Institute of Electrical and Electronics Engineers Inc., 445 Hoes Lane / P.O. Box 1331, Piscataway, NJ 08855-1331, United States

Abstract: We present a chip architecture for a compressive sensing based method that can be used in conjunction with the JTAG standard to detect IC Trojans. The proposed architecture compresses chip output resulting from a large number of test vectors applied to a circuit under test (CUT). We describe our designs in sensing leakage power, computing random linear combinations under compressive sensing, and piggybacking these new functionalities on JTAG. Our architecture achieves approximately a 10× speedup and 1000× reduction in output bandwidth while incurring a small area overhead. © 2012 IEEE.

Number of references: 19
Main heading: Signal reconstruction
Controlled terms: Electrical engineering - Signal processing
Uncontrolled terms: Chip architecture - Circuit under test - Compressive sensing - CS-JTAG - Leakage power - Linear combinations - Proposed architectures - Trojans
Classification code: 709 Electrical Engineering, General - 716.1 Information Theory and Signal Processing
DOI: 10.1109/SiPS.2012.33
Database: Compendex

Data Provider: Engineering Village