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

1. Power supply signal calibration techniques for improving detection resolution to hardware trojans

Accession number: 20085211818829
Authors: Rad, Reza M. (1); Wang, Xiaoxiao (2); Tehranipoor, Mohammad (2); Plusquellic, Jim (3)
Author affiliation: (1) Department of CSEE, Univ. of Maryland, Baltimore Campus; (2) Department of Electrical and Computer Engineering, Univ. of Connecticut; (3) Department of Electrical and Computer Engineering, Univ. of New Mexico
Corresponding author: Rad, R. M.
Source title: IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD
Abbreviated source title: IEEE ACM Int. Conf. Comput. Des. Dig. Tech. Pap. ICCAD
Monograph title: 2008 IEEE/ACM International Conference on Computer-Aided Design Digest of Technical Papers, ICCAD 2008
Issue date: 2008
Publication year: 2008
Pages: 632-639
Article number: 4681643
Language: English
ISSN: 10923152
CODEN: DICDFD
ISBN-13: 9781424428205
Document type: Conference article (CA)
Conference name: 2008 International Conference on Computer-Aided Design, ICCAD
Conference date: November 10, 2008 - November 13, 2008
Conference location: San Jose, CA, United states
Conference code: 74849
Sponsor: IEEE CAS/CANDE; IEEE Circuits and Systems Society; CANDE; ACM; SIGDA; CEDA
Publisher: Institute of Electrical and Electronics Engineers Inc., 3 Park Avenue, 17th Floor, New York, NY 10016-5997, United States
Abstract: Chip design and fabrication is becoming increasingly vulnerable to malicious activities and alternations with globalization. An adversary can introduce a Trojan designed to disable and/or destroy a system at some future time (Time Bomb) or the Trojan may serve to leak confidential information covertly to the adversary. This paper proposes a taxonomy for Trojan classification and then describes a statistical approach for detecting hardware Trojans that is based on the analysis of an ICs power supply transient signals. A key component to improving the resolution of power analysis techniques to Trojans is calibrating for process and test environment (PE) variations. The main focus of this research is on the evaluation of four signal calibration techniques, each designed to reduce the adverse impact of PE variations on our statistical Trojan detection method.
Number of references: 17
Main heading: Electric power distribution
Controlled terms: Calibration - Computer aided design - Electric power transmission networks - Electric power utilization - Integrated circuits - Taxonomies
Uncontrolled terms: Chip designs - Confidential informations - Detection methods - Key components - Malicious activities - Power analysis - Power supplies - Signal calibrations - Statistical approaches - Test environments - Transient signals - Trojans
Classification code: 943 Mechanical and Miscellaneous Measuring Instruments - 942 Electric and Electronic Measuring Instruments - 941 Acoustical and Optical Measuring Instruments - 903 Information Science - 902.2 Codes and Standards - 944 Moisture, Pressure and Temperature, and Radiation Measuring Instruments - 723.5 Computer Applications - 706.1.2 Electric Power Distribution - 706.1.1 Electric Power Transmission - 706.1 Electric Power Systems - 703.1 Electric Networks - 714.2 Semiconductor Devices and Integrated Circuits
DOI: 10.1109/ICCAD.2008.4681643
Database: Compendex

Data Provider: Engineering Village

1. Hardware Trojans: current challenges and approaches

Accession number: 14738830
Authors: Jacob, N. (1); Merli, D. (1); Heyszl, J. (1); Sigl, G. (1)
Author affiliation: (1) Fraunhofer AISEC, Garching, Germany
Source title: IET Computers & Digital Techniques
Abbreviated source title: IET Comput. Digit. Tech. (UK)
Volume: 8
Issue: 6
Publication date: Nov. 2014
Pages: 264-73
Language: English
ISSN: 1751-8601
CODEN: ICDTA6
Document type: Journal article (JA)
Publisher: IET
Country of publication: UK
Material Identity Number: DW19-2014-005
Abstract: More and more manufacturers outsource parts of the design and fabrication of integrated circuits (ICs) for cost reduction. Recent publications show that such outsourcing can pose serious threats to governments and corporations, as they lose control of the development process. Until now, the threat of hardware Trojans is mostly considered during fabrication. Third party intellectual properties (IPs) are also gaining importance as companies wish to reduce costs and shorten the time-to-market. Through this study, the authors argue that the threat of Trojans is spread throughout the whole IC development chain. They give a survey of both hardware Trojan insertion possibilities and detection techniques. Furthermore, they identify the key vulnerabilities at each stage of IC development and describe costs of hardware Trojan insertion and detection. This way, the threat level based on feasibility of Trojan insertion and the practicability of Trojan detection techniques is evaluated. Lately, detection techniques address the issue of including third party IP. However, those techniques are not sufficient and need more research to effectively protect the design. In this way, the authors' analysis provides a solid base to identify the issues during IC development, which should be addressed with higher priority by all entities involved in the IC development.
Number of references: 48
Inspec controlled terms: integrated circuits - invasive software
Uncontrolled terms: Trojan detection techniques - Trojan insertion - detection techniques - IC development chain - IP - intellectual properties - cost reduction - manufacturers outsource parts - Hardware Trojans
Inspec classification codes: B2220 Integrated circuits - C6130S Data security
Treatment: Practical (PRA)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
DOI: 10.1049/iet-cdt.2014.0039
IPC Code: G06F21/00
Database: Inspec

Data Provider: Engineering Village

1. Tutorial T4: All You Need to Know about Hardware Trojans and Counterfeit ICs

Accession number: 14126683
Authors: Tehranipoor, M. (1); Forte, D. (1)
Author affiliation: (1) Univ. of Connecticut, Storrs, CT, United States
Source: 2014 27th International Conference on VLSI Design and 2014 13th International Conference on Embedded Systems
Publication date: 2014
Pages: 9-10
Language: English
ISBN-13: 978-1-4799-2512-4
Document type: Conference article (CA)
Conference name: 2014 27th International Conference on VLSI Design and 2014 13th International Conference on Embedded Systems
Conference date: 5-9 Jan. 2014
Conference location: Mumbai, India
Sponsor: IEEE Comput. Soc.
Publisher: IEEE Computer Society
Place of publication: Los Alamitos, CA, USA
Material Identity Number: YXB4-1900-332
Abstract: The migration from a vertical to horizontal business model has made it easier to introduce hardware Trojans and counterfeit electronic parts into the electronic component supply chain. Hardware Trojans are malicious modifications made to original IC designs that reduce system integrity (change functionality, leak private data, etc.). Counterfeit parts are often below specification and/or of substandard quality. The existence of Trojans and counterfeit parts creates risks for the life-critical systems and infrastructures that incorporate them including automotive, aerospace, military, and medical systems. In this tutorial, we will cover: (i) Background and motivation for hardware Trojan and counterfeit prevention/detection; (ii) Taxonomies related to both topics; (iii) Existing solutions; (iv) Open challenges; (v) New and unified solutions to address these challenges.
Number of references: 0
Inspec controlled terms: hardware-software codesign - integrated circuit testing - invasive software
Uncontrolled terms: counterfeit IC - counterfeit detection - counterfeit prevention - life-critical systems - system integrity - original IC designs - electronic component supply chain - counterfeit electronic parts - hardware Trojans - horizontal business model - vertical business model
Inspec classification codes: B2570A Semiconductor integrated circuit design, layout, modelling and testing - B1265A Digital circuit design, modelling and testing - C5215 Hardware-software codesign - C5210 Logic design methods - C6130S Data security
Treatment: Practical (PRA)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
DOI: 10.1109/VLSID.2014.119
IPC Code: G01R31/28 - G06F21/00
Database: Inspec

Data Provider: Engineering Village

1. Hardware Trojans in wireless cryptographic ICs: Silicon demonstration & detection method evaluation

Accession number: 13999815
Authors: Yu Liu (1); Yier Jin (2); Makris, Y. (1)
Author affiliation: (1) Dept. of Electr. Eng., Univ. of Texas at Dallas, Dallas, TX, United States; (2) Dept. of Electr. Eng. & Comput. Sci., Univ. of Central Florida, Orlando, FL, United States
Source: 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)
Publication date: 2013
Pages: 399-404
Language: English
ISBN-13: 978-1-4799-1071-7
Document type: Conference article (CA)
Conference name: 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)
Conference date: 18-21 Nov. 2013
Conference location: San Jose, CA, USA
Sponsor: IEEE Counc. Electron. Design Autom.
Publisher: IEEE
Place of publication: Piscataway, NJ, USA
Material Identity Number: YXB4-1900-035
Abstract: We present a silicon implementation of a hardware Trojan, which is capable of leaking the secret key of a wireless cryptographic integrated circuit (IC) consisting of an Advanced Encryption Standard (AES) core and an Ultra-Wide-Band (UWB) transmitter. With its impact carefully hidden in the transmission specification margins allowed for process variations, this hardware Trojan cannot be detected by production testing methods of either the digital or the analog part of the IC and does not violate the transmission protocol or any system-level specifications. Nevertheless, the informed adversary, who knows what to look for in the transmission power waveform, is capable of retrieving the 128-bit AES key, which is leaked with every 128-bit ciphertext block sent by the UWB transmitter. Using silicon measurements from 40 chips fabricated in TSMC's 0.35µm technology, we also assess the effectiveness of a side channel-based statistical analysis method in detecting this hardware Trojan.
Number of references: 14
Inspec controlled terms: cryptography - invasive software - microprocessor chips - radio transmitters - radiofrequency integrated circuits - statistical analysis - ultra wideband communication
Uncontrolled terms: hardware trojans - wireless cryptographic IC - wireless cryptographic integrated circuit - silicon demonstration method evaluation - silicon detection method evaluation - secret key - advanced encryption standard core - ultra-wide-band transmitter - UWB transmitter - transmission specification margins - process variations - transmission power waveform - 128-bit AES key - TSMC 0.35µm technology - side channel-based statistical analysis method - silicon measurements - 128- bit ciphertext block
Inspec classification codes: B1350H Microwave integrated circuits - B2570 Semiconductor integrated circuits - B6250 Radio links and equipment - B6120D Cryptography - B1265F Microprocessors and microcomputers - B0240Z Other topics in statistics
Treatment: Practical (PRA); Theoretical or Mathematical (THR)
Discipline: Electrical/Electronic engineering (B)
DOI: 10.1109/ICCAD.2013.6691149
IPC Code: G06F15/76 - H01L27/00 - H04B1/02 - H04B7/00 - H04L9/00 - H04W - H04W84/18 - H04B1/7163
Database: Inspec

Data Provider: Engineering Village

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

1. Improving IC Security Against Trojan Attacks Through Integration of Security Monitors

Accession number: 13250677
Authors: Narasimhan, S. (1); Wen Yueh (2); Xinmu Wang (1); Mukhopadhyay, S. (2); Bhunia, S. (1)
Author affiliation: (1) EECS Dept., Case Western Reserve Univ., Cleveland, OH, United States; (2) Dept. of ECE, Georgia Tech, Atlanta, GA, United States
Source title: IEEE Design & Test of Computers
Abbreviated source title: IEEE Des. Test Comput. (USA)
Volume: 29
Issue: 5
Publication date: Oct. 2012
Pages: 37-46
Language: English
ISSN: 0740-7475
CODEN: IDTCEC
Document type: Journal article (JA)
Publisher: IEEE Computer Society
Country of publication: USA
Material Identity Number: CL78-2013-001
Abstract: This paper describes using on-chip monitors to significantly improve the sensitivity of side-channel signal analysis techniques to malicious inclusions in integrated circuits known as hardware Trojans.
Number of references: 12
Inspec controlled terms: electronic engineering computing - integrated circuit design - invasive software - system-on-chip
Uncontrolled terms: IC security improvement - on-chip monitors - side-channel signal analysis technique sensitivity - integrated circuits - hardware Trojans
Inspec classification codes: B1265M System-on-chip - B1265A Digital circuit design, modelling and testing - C7410D Electronic engineering computing - C6130S Data security - C5137 System-on-chip
Treatment: Practical (PRA)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
DOI: 10.1109/MDT.2012.2210183
IPC Code: G06F15/76 - G06F21/00
Database: Inspec

Data Provider: Engineering Village

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

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

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