2018 IEEE 3rd International Verification and Security Workshop (IVSW 2018)

Costa Brava, Spain
2 – 4 July 2018

IEEE Catalog Number: CFP18G73-POD
ISBN: 978-1-5386-6545-9

**Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP18G73-POD
ISBN (Print-On-Demand):	978-1-5386-6545-9
ISBN (Online):	978-1-5386-6544-2

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

Technical Papers

- Towards Self-Explaining Digital Systems: A Design Methodology for the Next Generation.....1
  Rolf Drechsler , Christoph Lüth , Goerschwin Fey and Tim Güneysu
- Detecting Cache-timing Vulnerabilities in Post-quantum Cryptography Algorithms.....7
  Adrien Facon, Sylvain Guilley, Matthieu Lec'Hvien , Alexander Schaub and Youssef Souissi
- Reverse Engineering of Cryptographic Cores by Structural Interpretation through Graph Analysis.....13
  Michael Werner, Bernhard Lippmann, Johanna Baehr and Helmut Grä
- Software-only Reverse Engineering of Physical DRAM Mappings for Rowhammer Attacks.....19
  Alessandro Barenghi, Luca Breveglieri, Niccolò Izzo and Gerardo Pelosi
- Authentication of Microcontroller Board Using Non-invasive EM Emission Technique.....25
  Mosabbah Mushir Ahmed, David Hely, Etienne Perret, Nicolas Barbot, Romain Siragusa, Maxime Bernier and Fredric Garet
- On the Mitigation of Hardware Trojan Attacks in Embedded Processors by Exploiting a Hardware-based Obfuscator.....31
  Andrea Marcelli, Ernesto Sanchez, Luca Sasselli and Giovanni Squillero
- Lightweight PUF-Based Authentication Protocol for IoT Devices.....38
  Yildiran Yilmaz, Steve R. Gunn and Basel Halak
- Security Analysis of Chaotic Baker Maps.....44
  Amira Elhamshary, Yehea Ismail and Said Elkhamy
- Architectural Diversity: Bio-Inspired Hardware Security for FPGAs.....48
  Shakil Mahmud, Brooks Olney and Robert Karam
- A Machine Learning Attacks Resistant Two Stage Physical Unclonable Functions Design.....52
  Haibo Su, Mark Zwolinski and Basel Halak
- Hardware Trojan Detection and Functionality Determination for Soft IPs.....56
  Thao Le, Lucas Weaver, Jia Di, Shaojie Zhang and Yier Jin
- Property Based Formal Security Verification for Hardware Trojan Detection.....62
  Maoyuan Qin, Wei Hu, Dejun Mu and Yu Tai
- A New Secure Stream Cipher for Scan Chain Encryption.....68
  Mathieu Da Silva, Emanuele Valea, Marie-Lise Flottes, Sophie Dupuis, Giorgio Di Natale and Bruno Rouzeyre
- Pre-silicon Embedded System Evaluation as new EDA Tool for Security Verification.....74
  Sofiane Takarabt, Kais Chibani, Adrien Facon, Sylvain Guilley, Yves Mathieu, Laurent Sauvage and Youssef Souissi
- Using Physical and Functional Comparisons to Assure 3rd-Party IP for Modern FPGAs.....80
  Adam Hastings, Sean Jensen, Jeffrey Goeders and Brad Hutchings
- Hardware Security Evaluation Platform for MCU-based Connected Devices: Application to healthcare IoT.....87
  Zahra Kazemi, Athanasios Papadimitriou, David Hely, Mahdi Fazeli and Vincent Beroulle
- Physical Inspection & Attacks: New Frontier in Hardware Security.....93
  M Tanjidur Rahman, Qihang Shi, Shahin Tajik, Haoting Shen, Damon L. Woodard, Mark Tehranipoor and Navid Asadizanjani