2017 IEEE 2nd International Verification and Security Workshop (IVSW 2017)

Thessaloniki, Greece
3-5 July 2017

IEEE Catalog Number: CFP17G73-POD
ISBN: 978-1-5386-1709-0

Copyright © 2017 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:	CFP17G73-POD
ISBN (Print-On-Demand):	978-1-5386-1709-0
ISBN (Online):	978-1-5386-1708-3

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

Session 2	Fault Injection / Side-Channel Attacks and Resistance
Date/Time	Monday, 3 July 2017 / 11:00 – 12:00

2-1 **Practical Evaluation of Masking Software Countermeasures on an IoT processor** 1
David McCann and Elisabeth Oswald

2-2 **Towards Mixed Structural-functional Models for Algebraic Fault Attacks on Ciphers** 7
Jan Burchard, Ange-Salomé Messeng Ekossono, Jan Horáček, Maël Gay, Bernd Becker, Tobias Schubert, Martin Kreuzer and Ilia Polian

2-3 **Robust Secure Design by Increasing the Resilience of Attack Protection Blocks 13**
Seyed-Abdollah Aftabjahani and Amitabh Das

Session 3	Physical Unclonable Functions and True Random Number Generators
Date/Time	Monday, 3 July 2017 / 12:00 – 12:40

3-1 **Lightweight Obfuscation Techniques for Modeling Attacks Resistant PUFs** 19
Mohd Syafiq Mispan, Basel Halak and Mark Zwolinski

3-2 **Entropy Justification for Metastability Based Nondeterministic Random Bit Generator** 25
Rachael J. Parker

Session 4	Special Session on Business Issues Related to Security
Date/Time	Monday, 3 July 2017 / 14:00 – 15:00

4-1 **Cross-Domain Cyber-Physical Systems Security - Case Study Manufacturing Supply Chain Security** N/A
Mohammad Abdullah Al Faruque

4-2 **Why open source hardware matters and why you should care N/A**
Frank K. Gürkaynak

4-3 **Open-Security Platforms to fill the gap between HW and SW security N/A**
Giuseppe Airo' Farulla, Paolo Prinetto and Antonio Varialle

Session 5	Special Session on Asynchronous Circuit Design for Security
Date/Time	Monday, 3 July 2017 / 15:15 – 16:15

5-1 **Self-Timed Ring Based True Random Number Generator: Threat Model and Countermeasures** 31
Grégoire Gimenez, Abdelkarim Cherkaoui, Raphael Frisch and Laurent Fesquet

5-2 **Reliable Communication across Parallel Asynchronous Channels with Glitches: Theory and Simulations** N/A
Shlomo Engelberg, Avri Horowitz and Hagay Zusman

5-3 **Security Aware Pseudo-Asynchronous Circuit Design Style N/A**
Itamar Levi, Alexander Fish and Osnat Keren

Session 6	Innovations in Cryptography and Control Flow Integrity
Date/Time	Monday, 3 July 2017 / 16:45– 18:15

6-1 **Provable Secure Dual-Server Public Key Encryption with Keyword Search** 39
Kaibin Huang and Raylin Tso

6-2 **Experimentations on Scan Chain Encryption with PRESENT** 45
Mathieu Da Silva , Marie-lise Flottes, Giorgio Di Natale and Bruno Rouzeyre

6-3 **Hacking the Control Flow Error Detection Mechanism** 51
Giorgio Di Natale, Marie-Lise Flottes , Sophie Dupuis and Bruno Rouzeyre

6-4 **A Red Team Blue Team approach Towards a Secure Processor Design With Hardware Shadow Stack** 57
Cyril Bresch, Adrien Michelet, Laurent Amato, Thomas Meyer and David Hely

Session 7	Panel : Challenges in IC Reverse and Anti-Reverse Engineering
Date/Time	Monday, 3 July 2017 / 18:30 – 19:30

Panelist
Michal Odstrcil , *Paul Scherrer Institut*
Shahin Tajik, *TU Berlin*
Olivier Thomas, *Texplained*
Johanna Baehr, *TU Munich*

Organizer & Moderator
Domenic Forte, *University of Florida*

Session 9	Emerging Design Challenges for Complex SoCs
Date/Time	Tuesday, 4 July 2017 / 09:45 – 10:45

Abstract

The increasing demand for electronic systems with increasing bandwidth and decreasing size puts more high-speed circuitry and high bandwidth channels in ever-closer proximity. System-on-a-chip (SoC) integration places complex high speed digital circuitry, analog and RF blocks very closely together. Note that most EDA tools are geared for a specific design type (digital, analog, RF, etc.) However, there are many challenges caused by the interaction across various blocks. These challenges are not limited by the boundaries or types of the various design components, or by the types of analyses that designers are used to regularly run on less complex homogenous designs. Most notable among these interdisciplinary mixed signal SOC challenges include:

- Verification of behavioral and electrical correctness
- Security verification
- Electromagnetic Crosstalk interference analysis and signoff

Panelist

Jacob Abraham , *Univ. of Texas at Austin*
Antonio Acosta, *Univ. of Seville*
Abhijit Chatterjee, *Georgia Tech*
Bozena Kaminska, *Simon Fraser Univ*
Padelis Papadopoulos, *Helic*

Linda Milor, *Georgia Tech*
Antonio Rubio, *UPC*

Moderator
Magdy Abadir, *Helic*

Organizers
Magdy Abadir & Manuel Barragan

Session 10	Continuous Monitoring for Faults, Attacks and Malware
Date/Time	Tuesday, 4 July 2017 / 11:15 – 12:15

10-1 **SNIFFER: A High-Accuracy Malware Detector for Enterprise-Based Systems** 70
Evan Chavis, Harrison Davis, Yijun Hou, Matthew Hicks, Salessawi Ferede Yitbarek, Todd Austin and Valeria Bertacco

10-2 **Hardware Performance Counters for System Reliability Monitoring** **76**
Elena Woo Lai Leng, Mark Zwolinski and Basel Halak

10-3 **Estimating Target Distribution in Security Assessment Models** 82
Eli Weintraub

Session 11	Special Session on Hardware Reverse Engineering and Implementation Attacks
Date/Time	Wednesday, 5 July 2017 / 13:30 – 14:30

11-1 **The Technology Impact on Laser Fault Injection** N/A
Falk Schellenberg and Christof Paar

11-2 **Hardware Reverse Engineering: Overview and Open Challenges** 88
Marc Fyrbiak, Sebastian Strauß, Christian Kison, Sebastian Wallat, Malte Elson, Nikol Rummel and Christof Paar

11-3 **A Look at the Dark Side of Hardware Reverse Engineering – A Case Study** 95
Sebastian Wallat, Marc Fyrbiak, Moritz Schlögel and Christof Paar

Session 13	IVSW Keynote 3 (Joint with IMTSW)
Date/Time	Wednesday, 5 July 2017 / 09:30 – 10:30
Moderator	S.Nikolaidis , *(Aristotle U Thessaloniki))*

13-1 **Secure Authentication of Electronic Systems with Autonomous Optical Nano-Devices** 107
Bozena Kaminska, Jasbir Patel and Hao Jiang

Session 14	Formal Verification and Design
Date/Time	Wednesday, 5 July 2017 / 10:45 – 11:25

14-1 **Learning Lemma Support Graphs in Quip and IC3** 111
Ryan Berryhill, Neil Veira, Andreas Veneris and Zissis Poulos

14-2 **Asserting Causal Properties in High Level Synthesis** **117**
Erwan Fabiani, Loïc Lagadec, Mohamed Ben Hammouda and Ciprian Teodorov

Session 15	Industry Session on FPGA Security/td>
Date/Time	Wednesday, 5 July 2017 / 11:50 – 12:30
Moderator	C.Lopez-Ongil , *(U Carlos III de Madrid)*

15-1 **Security of FPGAs in Data Centers** 123
Steve Trimberger and Steve McNeil

15-2 **Protecting Partial Regions in FPGA Bitstreams** 129
Karen Horovitz, Meha Kainth and Ryan Kenny

Session 16	Security Considerations in Advanced memories
Date/Time	Tuesday, 4 July 2017 / 15:00 – 15:40

16-1 **Design Considerations for Spintronic-based Security Primitives** **N/A**
Elena Ioana Vatajelu

16-2 **Zero Bit-Error-Rate Weak PUF based on Spin-Transfer-Torque MRAM Memories** 101
Elena Ioana Vatajelu, Giorgio Di Natale and Paolo Prinetto

17-1 Opening Pandora's Box: Implication of RLUT on Secure FPGA Applications and IP Security 134
Debapriya Basu Roy, Shivam Bhasin, Ivica Nikolić and Debdeep Mukhopadhyay

17-2 Maximizing the Throughput of Threshold-protected AES-GCM Implementations on FPGA 140
Jo Vliegen, Oscar Reparaz and Nele Mentens

17-3 Efficient design of Oscillator based Physical Unclonable Functions on Flash FPGAs 146
Ugo Mureddu, Oto Petura, Nathalie Bochard, Lilian Bossuet and Viktor Fischer

Additional Paper:

Challenges and Trends in SOC Electromagnetic(EM) Crosstalk 63

Padelis Papadopoulos, Anand Raman, Yorgos Koutsoyannopoulos, Nikolas Provatas, and Magdy Abadir,