2013 IEEE International Symposium on Hardware-Oriented Security and Trust

(HOST 2013)

Austin, Texas, USA
2 – 3 June 2013

IEEE Catalog Number: CFP13HOA-POD
ISBN: 978-1-4799-0559-1

Table of Contents

Session	**Academic Keynote**
Date/Time	Sunday, 2 June 2013 / 09:00 – 10:00
Speaker	**Prof. Dr. Ing. Ahmad-Reza Sadeghi** *Professor at Technische Universität Darmstadt and Scientific Director of Fraunhofer Institute for Secure Information Systems (SIT), and Director of Intel-TU Darmstadt Security Institute*
Chair	Michael Hsiao

Session	**Physically Unclonable Functions I**
Date/Time	Sunday, 2 June 2013 / 10:20 – 11:35
Chair	Ingrid Verbauwhede

Cloning Physically Unclonable Functions 1
Clemens Helfmeier, Christian Boit, Dmitry Nedospasov and Jean-Pierre Seifert

Intellectual Property Protection for FPGA Designs with Soft Physical Hash Functions: First Experimental Results 7
Stéphanie Kerckhof, François Durvaux, François-Xavier Standaert and Benoît Gérard

Novel Strong PUF based on Nonlinearity of MOSFET Subthreshold Operation 13
Mukund Kalyanaraman and Michael Orshansky

Session	**Poster Session**
Date/Time	Sunday, 2 June 2013 / 01:00 – 02:00

Localized Electromagnetic Analysis of RO PUFs 19
Dominik Merli, Johann Heyszl, Benedikt Heinz, Dieter Schuster, Frederic Stumpf and Georg Sigl

Enhancing Fault Sensitivity Analysis Through Templates 25
Filippo Melzani and Andrea Palomba

Hardware Implementations of the WG-5 Cipher for Passive RFID Tags 29
Mark D. Aagaard, Guang Gong and Rajesh K. Mota

Adapting Voltage Ramp-Up Time for Temperature Noise Reduction on Memory-Based PUFs 35
Mafalda Cortez, Said Hamdioui, Vincent van der Leest, Roel Maes and Geert-Jan Schrijen

Model Building Attacks on Physically Unclonable Functions using Genetic Programming 41
Indrasish Saha, Ratan Rahul Jeldi and Rajat Subhra Chakraborty

BISA: Built-In Self-Authentication for Preventing Hardware Trojan Insertion 45
Kan Xiao and Mohammed Tehranipoor

A Bulk Built-In Sensor for Detection of Fault Attacks 51
R. Possamai Bastos, F. Sill Torres, J.-M. Dutertre, M.-L. Flottes, G. Di Natale and B. Rouzeyre

Session	**Obfuscation and Identification**
Date/Time	Sunday, 2 June 2013 / 02:20 – 03:35
Chair	William Robinson

Structural Transformation for Best-Possible Obfuscation of Sequential Circuits 55
Li Li and Hai Zhou

An Efficient Algorithm for Identifying Security Relevant Logic and Vulnerabilities in RTL Designs 61
David W. Palmer and Parbati Kumar Manna

WordRev: Finding Word-Level Structures in a Sea of Bit-Level Gates 67
Wenchao Li, Adria Gascon, Pramod Subramanyan, Wei Yang Tan, Ashish Tiwari, Sharad Malik, Natarajan Shankar and Sanjit A. Seshia

Session	**Novel Implementations**
Date/Time	Sunday, 2 June 2013 / 04:00 – 05:40
Chair	Francesco Regazzoni

On Implementing Trusted Boot for Embedded Systems 75
Obaid Khalid, Carsten Rolfes and Andreas Ibing

Low-Cost and Area-Efficient FPGA Implementations of Lattice-Based Cryptography 81
Aydin Aysu, Cameron Patterson and Patrick Schaumont

Design and Implementation of Rotation Symmetric S-Boxes with High Nonlinearity and High DPA Resilience 87
Bodhisatwa Mazumdar, Debdeep Mukhopadhyay and Indranil Sengupta

On-chip Lightweight Implementation of Reduced NIST Randomness Test Suite 93
Vikram B. Suresh, Daniele Antonioli and Wayne P. Burleson

Session	**Hardware Trojans**
Date/Time	Monday, 3 June 2013 / 08:45 – 10:00
Chair	Swarup Bhunia

Cycle-Accurate Information Assurance by Proof-Carrying Based Signal Sensitivity Tracing 99
Yier Jin, Bo Yang and Yiorgos Makris

On Hardware Trojan Design and Implementation at Register-Transfer Level 107
Jie Zhang and Qiang Xu

Malicious Circuitry Detection Using Fast Timing Characterization via Test Points 113
Sheng Wei and Miodrag Potkonjak

Session	**Industrial Keynote**
Date/Time	Monday, 3 June 2013 / 10:20 – 11:30
Speaker	**Ron Cocchi**, *Vice President and CTO, Syphermedia International*
Chair	Ted Huffmire

Panel	**Panel on Industry Challenges for Hardware and Embedded Systems Security**
Date/Time	Monday, 3 June 2013 / 12:45 – 02:00

Session	**Side Channels**
Date/Time	Monday, 3 June 2013 / 02:00 – 03:15
Chair	Yiorgos Makris

Frontside Laser Fault Injection on Cryptosystems – Application to the AES' Last Round – 119
Cyril Roscian, Jean-Max Dutertre and Assia Tria

Side-Channel Analysis of MAC-Keccak 125
Mostafa Taha and Patrick Schaumont

Pre-Processing Power Traces with a Phase-Sensitive Detector 131
P. Hodgers, N. Hanley and M. O'Neill

Session	**Physically Unclonable Functions II**
Date/Time	Monday, 3 June 2013 / 03:30 – 04:45
Chair	Jean-Pierre Seifert

Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise 137
Jeroen Delvaux and Ingrid Verbauwhede

Stability Analysis of a Physical Unclonable Function Based on Metal Resistance Variations 143
J. Ju, R. Chakraborty, C. Lamech and J. Plusquellic

Error-Tolerant Bit Generation Techniques for use with a Hardware-Embedded Path Delay PUF **151**
J. Aarestad, J. Plusquellic and D. Acharyya