Preface

On behalf of the organizing, program, and steering committees, it is a great pleasure to welcome you to the 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2013). The HOST meeting is held as a co-located event at DAC 2013 in Austin, TX, June 2 and 3, 2013.

Now in its sixth installment, HOST has received high interest from several communities active in hardware-oriented security. This includes, among others, the embedded systems community, the microprocessor community, the ASIC design community, and the ASIC test community. HOST receives equal interest from the academic world as well as from industry.

This year HOST is receiving support from industry sponsors, emphasizing the increasingly important role of the symposium. We gratefully acknowledge the support from Intel and Microsemi. In addition, HOST receives support from several societies, including the IEEE Computer Society, IEEE Test Technology Technical Council, and IEEE Security and Privacy Society.

HOST received 62 regular submissions; 19 were accepted as a regular paper, and 7 were accepted as posters. This year, the review process followed the rigorous evaluation procedure adopted last year. First, each anonymously submitted paper was reviewed by at least five of the Program committee and organizing committee members. Next, the reviews were cross-verified in an on-line discussion among the PC and organizing committee members that did not have conflicts with the paper authors. This evaluation ensured that the reviews were consistent. Where needed, additional reviews were performed. The final decision of accepting or rejecting a paper was made by consensus among the reviewers. We thank the program and organizing committee for their efforts and their dedication to the quality of the HOST 2013 program.

The two-day program includes, besides the 19 regular presentations and the 7 poster presentations, keynotes by Dr. Ing Ahmad-Reza Sadeghi from TU Darmstadt and Fraunhofer, Dr. Ron Cocchi from Syphermedia International, Daniel DiMase from Honeywell, and Dennis Polla from IARPA. We also have a panel entitled Industry Challenges for Hardware and Embedded Systems Security.

Finally, we would like to thank members of the program committee, organizing committee, and steering committee for their efforts to make HOST more successful with each passing year.

Ramesh Karri, Polytechnic Institute of New York University
Farinaz Koushanfar, Rice University
Michael Hsiao, Virginia Tech
Steering and Program Committee

General Chair
R. Karri, Polytechnic Inst., New York University

Program Chair
F. Koushanfar, Rice University

Vice-Program Chair
M. Hsiao, Virginia Tech University

Past Program Chair
Ken Mai, Carnegie Mellon University

Publicity Chair
S. Bhunia, Case Western Reserve University

Publication Chair
Ted Huffmire, Naval Posgraduate School

Finance Chair
William Robinson, Vanderbilt University

Panel Chair
K. Mai, Carnegie Mellon University

Registration Chair
Jim Plusquellic, University of New Mexico

Co-Founders
Mohammad Tehranipoor, UConn
Jim Plusquellic, UNM

Steering Committee
Mohammad Tehranipoor, UConn (Chair)
Jim Plusquellic, UNM
Farinaz Koushanfar, Rice University
Miodrag Potkonjak, UCLA
Ken Mai, Carnegie Mellon University

Program Committee
Jim Plusquellic, University of New Mexico
Patrick Schaumont, Virginia Tech
Mohammad Tehranipoor, University of Connecticut
Kazuo Sakiyama, The University of Electro-Communications
Sylvain Guilley, GET/ENST, CNRS/LTCI
Pankaj Rohatgi, Cryptography Research
Ingrid Verbauwhede, KU Leuven, ESAT/COSIC
Ian Harris, University of California Irvine
Swarup Bhunia, Case Western Reserve University
Miodrag Potkonjak, University of California, Los Angeles
Francois-Xavier Standaert, UCL Crypto Group
Ken Mai, Carnegie Mellon University

2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)
# Table of Contents

<table>
<thead>
<tr>
<th>Session</th>
<th>Academic Keynote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Sunday, 2 June 2013 / 09:00 – 10:00</td>
</tr>
</tbody>
</table>
| 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 |

<table>
<thead>
<tr>
<th>Session</th>
<th>Physically Unclonable Functions I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Sunday, 2 June 2013 / 10:20 – 11:35</td>
</tr>
<tr>
<td>Chair</td>
<td>Ingrid Verbauwhede</td>
</tr>
</tbody>
</table>

- Cloning Physically Unclonable Functions  
* Clemens Helfmeier, Christian Boit, Dmitry Nedospasov and Jean-Pierre Seifert
- Intellectual Property Protection for FPGA Designs with Soft Physical Hash Functions: First Experimental Results  
* Stéphanie Kerckhof, François Durvaux, François-Xavier Standaert and Benoît Gérard
- Novel Strong PUF based on Nonlinearity of MOSFET Subthreshold Operation  
* Mukund Kalyanaraman and Michael Orshansky

<table>
<thead>
<tr>
<th>Session</th>
<th>Poster Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Sunday, 2 June 2013 / 01:00 – 02:00</td>
</tr>
</tbody>
</table>

- Localized Electromagnetic Analysis of RO PUFs  
* Dominik Merli, Johann Heyszl, Benedikt Heinz, Dieter Schuster, Frederic Stumpf and Georg Sigl
- Enhancing Fault Sensitivity Analysis Through Templates  
* Filippo Melzani and Andrea Palomba
- Hardware Implementations of the WG-5 Cipher for Passive RFID Tags  
* Mark D. Aagaard, Guang Gong and Rajesh K. Mota
- Adapting Voltage Ramp-Up Time for Temperature Noise Reduction on Memory-Based PUFs  
* Mafalda Cortez, Said Hamdioui, Vincent van der Leest, Roel Maes and Geert-Jan Schrijen
- Model Building Attacks on Physically Unclonable Functions using Genetic Programming  
* Indrasish Saha, Ratan Rahul Jeldi and Rajat Subhra Chakraborty
- BISA: Built-In Self-Authentication for Preventing Hardware Trojan Insertion  
* Kan Xiao and Mohammed Tehranipoor
- A Bulk Built-In Sensor for Detection of Fault Attacks  

---

2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)
<table>
<thead>
<tr>
<th>Session</th>
<th>Obfuscation and Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Sunday, 2 June 2013 / 02:20 – 03:35</td>
</tr>
<tr>
<td>Chair</td>
<td>William Robinson</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Session</th>
<th>Novel Implementations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Sunday, 2 June 2013 / 04:00 – 05:40</td>
</tr>
<tr>
<td>Chair</td>
<td>Francesco Regazzoni</td>
</tr>
</tbody>
</table>

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

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

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

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

<table>
<thead>
<tr>
<th>Session</th>
<th>Hardware Trojans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Monday, 3 June 2013 / 08:45 – 10:00</td>
</tr>
<tr>
<td>Chair</td>
<td>Swarup Bhunia</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Session</th>
<th>Industrial Keynote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Monday, 3 June 2013 / 10:20 – 11:30</td>
</tr>
<tr>
<td>Speaker</td>
<td>Ron Cocchi, <em>Vice President and CTO, Syphermedia International</em></td>
</tr>
<tr>
<td>Chair</td>
<td>Ted Huffmire</td>
</tr>
<tr>
<td>Panel</td>
<td>Panel on Industry Challenges for Hardware and Embedded Systems Security</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Monday, 3 June 2013 / 12:45 – 02:00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Session</th>
<th>Side Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Monday, 3 June 2013 / 02:00 – 03:15</td>
</tr>
<tr>
<td>Chair</td>
<td>Yiorgos Makris</td>
</tr>
</tbody>
</table>

- **Frontside Laser Fault Injection on Cryptosystems – Application to the AES’ Last Round**  
  Cyril Roscian, Jean-Max Dutertre and Assia Tria
- **Side-Channel Analysis of MAC-Keccak**  
  Mostafa Taha and Patrick Schaumont
- **Pre-Processing Power Traces with a Phase-Sensitive Detector**  
  P. Hodgers, N. Hanley and M. O'Neill

<table>
<thead>
<tr>
<th>Session</th>
<th>Physically Unclonable Functions II</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Monday, 3 June 2013 / 03:30 – 04:45</td>
</tr>
<tr>
<td>Chair</td>
<td>Jean-Pierre Seifert</td>
</tr>
</tbody>
</table>

- **Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise**  
  Jeroen Delvaux and Ingrid Verbauwhede
- **Stability Analysis of a Physical Unclonable Function Based on Metal Resistance Variations**  
  J. Ju, R. Chakraborty, C. Lamech and J. Plusquellic
- **Error-Tolerant Bit Generation Techniques for use with a Hardware-Embedded Path Delay PUF**  
  J. Aarestad, J. Plusquellic and D. Acharyya
## Author Index

**A**  
Aagaard, Mark D. 022  
Aarestad, J. 071  
Acharyya, D. 071  
Antonioli, Daniele 058  
Aysu, Aydin 033  

**B**  
Bastos, R. Possamai 053  
Boit, Christian 008  
Burleson, Wayne P. 058  

**C**  
Chakraborty, R. 070  
Chakraborty, Rajat Subhra 027  
Cortez, Mafalda 025  

**D**  
Delvaux, Jeroen 049  
Durvaux, François 042  
Dutertre, J. -M. 053  
Dutertre, Jean-Max 017  

**F**  
Flottes, M. -L. 053  

**G**  
Gérard, Benoît 042  
Gascon, Adria 077  
Gong, Guang 022  

**H**  
Hamdioui, Said 025  
Hanley, N. 047  
Heinz, Benedikt 004  
Helfmeier, Clemens 008  
Heyszl, Johann 004  
Hodgers, P. 047  

**I**  
Ibing, Andreas 018  

**J**  
Jeldi, Ratan Rahul 027  
Jin, Yier 039  
Ju, J. 070  

**K**  
Kalyanaraman, Mukund 061  
Kerckhof, Stéphanie 042  
Khalid, Obaid 018  

**L**  
Lamech, C. 070  
Leest, Vincent van der 025  
Li, Li 029  
Li, Wenchao 077  

**M**  
Maes, Roel 025  
Makris, Yiorgos 039  
Malik, Sharad 077  
Manna, Parbati Kumar 031  
Mazumdar, Bodhisatwa 040  
Melzani, Filippo 010  
Merli, Dominik 004  
Mota, Rajesh K. 022  
Mukhopadhyay, Debdeep 040  

**N**  
Natale, G. Di 053  
Nedospasov, Dmitry 008  

**O**  
O’Neill, M. 047  
Orshansky, Michael 061  

**P**  
Palmer, David W. 031  
Palomba, Andrea 010  
Patterson, Cameron 033  
Plusquellec, J. 070, 071  
Potkonjak, Miodrag 059  

**R**  
Rolfes, Carsten 018  
Roscian, Cyril 017  
Rouzeyre, B. 053  

**S**  
Saha, Indrasish 027  
Schaumont, Patrick 033, 036  
Schrijen, Geert-Jan 025  
Schuster, Dieter 004  
Seifert, Jean-Pierre 008  
Sengupta, Indranil 040  
Seshia, Sanjit A. 077  
Shankar, Natarajan 077  
Sigl, Georg 004  
Standaert, François-Xavier 042  
Stumpf, Frederic 004  
Subramanyan, Pramod 077  
Suresh, Vikram B. 058  

**T**  
Taha, Mostafa 036  
Tan, Wei Yang 077  
Tehranipoor, Mohammed 048  
Tiwari, Ashish 077  
Torres, F. Sill 053  
Tria, Assia 017  

**V**  
Verbauwhede, Ingrid 049  

**W**  
Wei, Sheng 059  

**X**  
Xiao, Kan 048  
Xu, Qiang 050  

**Y**  
Yang, Bo 039  

**Z**  
Zhang, Jie 050  
Zhou, Hai 029  

---

2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)