2013 IEEE International Symposium on Hardware-Oriented Security and Trust

(HOST 2013)

Austin, Texas, USA
2 – 3 June 2013
# 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>
<tr>
<td>Speaker</td>
<td>Prof. Dr. Ing. Ahmad-Reza Sadeghi</td>
</tr>
<tr>
<td></td>
<td><em>Professor at Technische Universität Darmstadt and Scientific Director of Fraunhofer Institute for Secure Information Systems (SIT), and Director of Intel-TU Darmstadt Security Institute</em></td>
</tr>
<tr>
<td>Chair</td>
<td>Michael Hsiao</td>
</tr>
</tbody>
</table>

<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>

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

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

3. **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>

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

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

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

35. **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

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

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

51. **A Bulk Built-In Sensor for Detection of Fault Attacks**
### 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**  
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

### Novel Implementations

#### Date/Time
Sunday, 2 June 2013 / 04:00 – 05:40

#### Chair
Francesco Regazzoni

**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

### 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**  
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

### Industrial Keynote

#### Date/Time
Monday, 3 June 2013 / 10:20 – 11:30

#### Speaker
Ron Cocchi, Vice President and CTO, Syphermedia International

#### Chair
Ted Huffmire
<table>
<thead>
<tr>
<th>Panel</th>
<th>Panel on Industry Challenges for Hardware and Embedded Systems Security</th>
</tr>
</thead>
<tbody>
<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*  
119

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

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

<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*  
137

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

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