

# **2011 IEEE International Symposium on Hardware-Oriented Security and Trust**

**(HOST 2011)**

**San Diego, California, USA  
5 – 6 June 2011**



**IEEE Catalog Number: CFP11HOA-PRT  
ISBN: 978-1-4577-1059-9**

# TABLE OF CONTENTS

## KEYNOTE

<b>Security Challenges and Opportunities in Adaptive and Reconfigurable Hardware .....</b>	<b>1</b>
<i>V. Costan, S. Devadas</i>	

## IP PROTECTION AND TROJAN DETECTION

<b>TinyTPM: A Lightweight Module aimed to IP Protection and Trusted Embedded Platforms .....</b>	<b>6</b>
<i>T. Feller, S. Malipatlolla, D. Meister, S. Huss</i>	
<b>Enhancing Security via Provably Trustworthy Hardware Intellectual Property .....</b>	<b>12</b>
<i>E. Lowe, Y. Jin, Y. Makris</i>	
<b>ODETTE: A Non-Scan Design-for-Test Methodology for Trojan Detection in ICs .....</b>	<b>18</b>
<i>M. Banga, M. Hsiao</i>	

## POSTER SESSION

<b>Influence of the Temperature on True Random Number Generators .....</b>	<b>24</b>
<i>M. Soucarros, C. Canovas-Dumas, J. Clediere, P. Elbaz-Vincent, D. Real</i>	
<b>Implementation and Verification of DPA-Resistant Cryptographic DES Circuit using Domino-RSL .....</b>	<b>28</b>
<i>K. Iwai, M. Shiozaki, A. Hoang, K. Kojima, T. Fujino</i>	
<b>Security Checkers: Detecting Processor Malicious Inclusions at Runtime .....</b>	<b>34</b>
<i>M. Bilzor, T. Huffmire, C. Irvine, T. Levin</i>	
<b>Formal Security Evaluation of Hardware Boolean Masking against Second-Order Attacks .....</b>	<b>40</b>
<i>H. Maghrebi, S. Guilley, J. Danger</i>	
<b>TrustGeM: Dynamic Trusted Environment Generation for Chip-Multiprocessors .....</b>	<b>47</b>
<i>L. Bathen, N. Dutt</i>	
<b>Performance Evaluation of Protocols Resilient to Physical Attacks .....</b>	<b>51</b>
<i>S. Guilley, L. Sauvage, J. Danger, N. Selmane, D. Real</i>	
<b>Flexible Architecture Optimization and ASIC Implementation of Group Signature Algorithm using a Customized HLS Methodology .....</b>	<b>57</b>
<i>S. Morioka, T. Isshiki, S. Obana, Y. Nakamura, K. Sako</i>	
<b>Systematic Security Evaluation Method Against C Safe-Error Attacks .....</b>	<b>63</b>
<i>D. Karaklajic, J. Fan, I. Verbauwheide</i>	
<b>Case Study: Detecting Hardware Trojans in Third-Party Digital IP Cores .....</b>	<b>67</b>
<i>X. Zhang, M. Tehranipoor</i>	
<b>TeSR: A Robust Temporal Self-Referencing Approach for Hardware Trojan Detection .....</b>	<b>71</b>
<i>S. Narasimhan, X. Wang, D. Du, R. Chakraborty, S. Bhunia</i>	

## METHODS FOR SIDE-CHANNEL ANALYSIS

<b>Algorithmic Collision Analysis for Evaluating Cryptographic Systems and Side-channel Attacks .....</b>	<b>75</b>
<i>Q. Luo, Y. Fei</i>	
<b>Accelerating Early Design Phase Differential Power Analysis Using Power Emulation Techniques .....</b>	<b>81</b>
<i>A. Krieg, C. Bachmann, J. Grinschgl, C. Steger, R. Weiss, J. Haid</i>	
<b>A Fast Power Current Analysis Methodology Using Capacitor Charging Model for Side Channel Attack Evaluation .....</b>	<b>87</b>
<i>D. Fujimoto, M. Nagata, T. Katashita, A. Sasaki, Y. Hori, A. Satoh</i>	

## SECURE ARCHITECTURE

<b>Hardware Security in Practice: Challenges and Opportunities .....</b>	<b>93</b>
<i>N. Potlapally</i>	

<b>Low-Cost Recovery For The Code Integrity Protection In Secure Embedded Processors</b> .....	99
<i>N. Huu, B. Robisson, M. Agoyan, N. Drach</i>	
<b>New Security Threats Against Chips Containing Scan Chain Structures</b> .....	105
<i>J. Rolt, G. Natale, M. Flottes, B. Rouzeyre</i>	

### **INDUSTRIAL SESSION**

<b>Placement of Trust Anchors in Embedded Computer Systems</b> .....	111
<i>S. Papa, W. Casper, S. Nair</i>	
<b>MARVEL - Malicious Alteration Recognition and Verification by Emission of Light</b> .....	117
<i>P. Song, F. Stellari, D. Pfeiffer, J. Culp, A. Weger, A. Bomoit, B. Wisnieff, M. Taubenblatt</i>	
<b>A Survey of Frequently Identified Vulnerabilities in Commercial Computing Semiconductors</b> .....	122
<i>K. Gotze</i>	

### **PHYSICAL UNCLONABLE FUNCTIONS**

<b>Hardware Intrinsic Security Based on SRAM PUFs: Tales from the Industry</b> .....	127
<i>H. Handschuh</i>	
<b>Reliable and Efficient PUF-Based Key Generation Using Pattern Matching</b> .....	128
<i>Z. Paral, S. Devadas</i>	
<b>The Bistable Ring PUF: A New Architecture for Strong Physical Unclonable Functions</b> .....	134
<i>Q. Chen, G. Csaba, U. Schlichtmann, U. Ruhmair, P. Lugli</i>	
<b>On Improving Reliability of Delay Based Physically Unclonable Functions under Temperature Variations</b> .....	142
<i>R. Kumar, H. Chandrikakutty, S. Kundu</i>	

### **SIDE-CHANNEL ATTACKS AND FAULT ATTACKS**

<b>Revisit Fault Sensitivity Analysis on WDDL-AES</b> .....	148
<i>Y. Li, K. Ohta, K. Sakiyama</i>	
<b>Practical Evaluation of DPA Countermeasures on Reconfigurable Hardware</b> .....	154
<i>A. Moradi, O. Mischke, C. Paar</i>	
<b>A Novel Fault Attack Against ECDSA</b> .....	161
<i>A. Barengi, G. Bertoni, A. Palomba, R. Susella</i>	
<b>Author Index</b>	