

2010 IEEE International Symposium on Hardware-Oriented Security and Trust

(HOST'2010)

**Anaheim, California, USA
13 – 14 June 2010**



**IEEE Catalog Number: CFP10HOA-PRT
ISBN: 978-1-4244-7811-8**

TABLE OF CONTENTS

SESSION 1 - ATTACKS

Entropy-based Power Attack	1
<i>H. Maghrebi, S. Guilley, J-L Danger, F. Flament</i>	
Low Voltage Fault Attacks to AES	7
<i>A. Barengi, G. Bertoni, L. Breveglieri, M. Pelliccioli, G. Pelosi</i>	
Multiple-Parameter Side-Channel Analysis: A Non-invasive Hardware Trojan Detection Approach	13
<i>S. Narasimhan, R. Chakraborty, D. Du, S. Paul, F. Wolff, C. Papachristou, Kaushik Roy, S. Bhunia</i>	

SESSION 2 - INDUSTRIAL

Anti-tamper JTAG TAP Design Enables DRM to JTAG Registers and P1687 onchip Instruments	19
<i>Cj Clark</i>	
Using Multiple Processors in a Single Reconfigurable Fabric for High-assurance Applications	25
<i>Bruce Newgard, Colby Hoffman</i>	

SESSION 3 - WATERMARKING

Side-channel based Watermarks for Integrated Circuits	30
<i>Georg T. Becker, Markus Kasper, Amir Moradi, Christof Paar</i>	
Multiplexing Methods for Power Watermarking	36
<i>Daniel Ziener, Florian Baueregger, Jürgen Teich</i>	
Provably Secure Obfuscation of Diverse Watermarks for Sequential Circuits	42
<i>Farinaz Koushanfar, Yousra Alkabani</i>	

SESSION 4 – POSTER SESSION

FPGA Implementations of the Hummingbird Cryptographic Algorithm	48
<i>Xinxin Fan, Guang Gong, Ken Lauffenburger, Troy Hicks</i>	
ExCCel: Exploration of Complementary Cells for Efficient DPA Attack Resistivity	52
<i>Kazuyuki Tanimura, Nikil Dutt</i>	
Trusted RTL: Trojan Detection Methodology in Pre-silicon Designs	56
<i>Mainak Banga, Michael S. Hsiao</i>	
Prototyping Platform for Performance Evaluation of SHA-3 Candidates	60
<i>Kazuyuki Kobayashi, Jun Ikegami, Kazuo Sakiyama, Kazuo Ohta, Miroslav Knežević, Ünal Kocabas, Junfeng Fan, Ingrid Verbauwhede, Eric Xu Guo, Shin'Ichiro Matsuo, Sinan Huang, Leyla Nazhandali, Akashi Satoh</i>	
A Comparison of Power-analysis-resistant Digital Circuits	64
<i>Eric Menendez, Ken Mai</i>	
SLICED: Slide-based Concurrent Error Detection Technique for Symmetric Block Ciphers	70
<i>Jeyavijayan Rajendran, Hetal Borad, Shyam Mantravadi, Ramesh Karri</i>	

SESSION 4 – ELLIPTIC CURVE CRYPTOGRAPHY

State-of-the-art of Secure ECC Implementations: A Survey on Known Sidechannel Attacks and Countermeasures	76
<i>Junfeng Fan, Xu Guo, Elke De Mulder, Patrick Schaumont, Bart Preneel, Ingrid Verbauwhede</i>	
Efficient One-pass Entity Authentication based on ECC for Constrained Devices	88
<i>Johann Heyszl, Frederic Stumpf</i>	

SESSION 5 – PHYSICAL UNCLONABLE FUNCTIONS

A Large Scale Characterization of RO-PUF	94
<i>Abhranil Maiti, Jeff Casarona, Luke McHale, Patrick Schaumont</i>	
LISA: Maximizing RO PUF's Secret Extraction	100
<i>Chi-En Daniel Yin, Gang Qu</i>	
Attack Resistant Sense Amplifier based PUFs (SA-PUF) with Deterministic and Controllable Reliability of PUF Responses Sensor Physical Unclonable Functions	106
<i>Kurt Rosenfeld, Efstratios Gavas, Ramesh Karri</i>	
Sensor Physical Unclonable Functions	112
<i>Kurt Rosenfeld, Efstratios Gavas, Ramesh Karri</i>	

SESSION 6 – IMPLEMENTATIONS AND COUNTERMEASURES

Current Flattening Circuit for DPA Countermeasure	118
<i>Ekarat Laohavaleeson, Chintan Patel</i>	
Side-channel Attack Resistant ROM-based AES S-Box	124
<i>Craig Teegarden, Mudit Bhargava, Ken Mai</i>	
Hardware Implementations of Hash Function Luffa	130
<i>Akashi Satoh, Toshihiro Katashita, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki</i>	
Entropy Extraction in Metastability-based TRNG	135
<i>Vikram B. Suresh, Wayne P. Burleson</i>	
Author Index	