

2012 IEEE International Symposium on Hardware-Oriented Security and Trust

(HOST 2012)

**San Francisco, California, USA
3 – 4 June 2012**



**IEEE Catalog Number: CFP12HOA-PRT
ISBN: 978-1-4673-2341-3**

TABLE OF CONTENTS

PHYSICALLY UNCLONABLE FUNCTIONS

Complementary IBS: Application Specific Error Correction for PUFs	1
<i>M. Hiller, D. Merli, F. Stumpf, G. Sigl</i>	
Buskeeper PUFs, a Promising Alternative to D Flip-Flop PUFs	7
<i>P. Simons, E. Sluis, V. Leest</i>	
Bit String Analysis of Physical Unclonable Functions based on Resistance Variations in Metals and Transistors	13
<i>J. Ju, J. Plusquellic, R. Chakraborty, R. Rad</i>	

POSTER SESSION

A Novel Method for Watermarking Sequential Circuits	21
<i>M. Lewandowski, R. Meana, M. Morrison, S. Katkooi</i>	
Reliability Enhancement of Bi-Stable PUFs in 65nm Bulk CMOS	25
<i>M. Bhargava, C. Cakir, K. Mai</i>	
SDMLp: On the Use of Complementary Pass Transistor Logic for Design of DPA Resistant Circuits	31
<i>L. Ramakrishnan, M. Chakkaravarthy, A. Manchanda, M. Borowczak, R. Vemuri</i>	
Register Leakage Masking Using Gray Code	37
<i>H. Maghrebi, S. Guilley, E. Prouff, J. Danger</i>	
An Adaptable, Modular, and Autonomous Side-Channel Vulnerability Evaluator	43
<i>M. Zohner, M. Stottinger, S. Huss, O. Stein</i>	
Evaluating Security Requirements in a General-Purpose Processor by Combining Assertion Checkers with Code Coverage	49
<i>M. Bilzor, T. Huffmire, C. Irvine, T. Levin</i>	
HTOutlier: Hardware Trojan Detection with Side-Channel Signature Outlier Identification	55
<i>J. Zhang, H. Yu, Q. Xu</i>	
FPGA Based Trustworthy Authentication Technique Using Physically Unclonable Functions and Artificial Intelligence	59
<i>S. Pappala, M. Niamat, W. Sun</i>	
t-Private Logic Synthesis on FPGAs	63
<i>J. Park, A. Tyagi</i>	

HARDWARE TROJANS

Interacting with Hardware Trojans Over a Network	69
<i>M. Farag, L. Lerner, C. Patterson</i>	
Trojan Detection based on Delay Variations Measured using a High-precision, Low-Overhead Embedded Test Structure	75
<i>C. Lamech, J. Plusquellic</i>	
Reverse Engineering Circuits Using Behavioral Pattern Mining	83
<i>W. Li, Z. Wasson, S. Seshia</i>	

COUNTERMEASURES I

Glitch-Free Implementation of Masking in Modern FPGAs	89
<i>A. Moradi, O. Mischke</i>	
A Systematic M Safe-error Detection in Hardware Implementations of Cryptographic Algorithms	96
<i>D. Karaklajic, J. Fan, I. Verbauwhede</i>	
Functional Integrated Circuit Analysis	102
<i>D. Nedospasov, J. Seifert, A. Schlosser, S. Orlic</i>	

**DANGERS OF COUNTERFEIT ELECTRONIC COMPONENTS DETECTION CHALLENGES,
SOLUTIONS AND POLICIES**

Performance Metrics and Empirical Results of a PUF Cryptographic Key Generation ASIC 108
M. Yu, R. Sowell, A. Singh, D. M'Raihl, S. Devadas

HSDL: A Security Development Lifecycle for Hardware Technologies 116
H. Khattri, N. Mangipudi, S. Mandujano

Design Solutions for Securing SRAM Cell Against Power Analysis..... 122
V. Rozic, W. Dehaene, I. Verbauwhe

On Charge Sensors for FIB Attack Detection 128
C. Helfmeier, C. Boit, U. Kerst

Detection of Probing Attempts in Secure ICs..... 134
S. Manich, M. Wamser, G. Sigl

SIDE-CHANNEL ATTACKS AND FAULT ATTACKS

Fault Round Modification Analysis of the Advanced Encryption Standard 140
J. Dutertre, A. Mirbaha, D. Naccache, A. Ribotta, A. Tria, T. Vaschale

Improved Algebraic Side-Channel Attack on AES..... 146
M. Mohamed, S. Bulygin, M. Zohner, A. Heuser, M. Walter, J. Buchmann

Author Index