HOST 2012

June 3-4, 2012
Moscone Center,
San Francisco, CA, USA

IEEE Sponsors

IEEE SECURITY&PRIVACY

tttc

IEEE computer society

Industry Sponsors

intel

Microsemi

Sunday – June 3, 2012

8:45 - 9:00: Opening Remarks
Ken Mai (CMU) and Ramesh Karri (NYU-Poly)

9:00 - 10:00: Keynote Speech
Session Chair: Ramesh Karri

Dr. Carl McCants, DARPA, TRUST

10:00 - 10:20: Break

10:20 - 11:35: Physically Unclonable Functions
Session Chair: Jorge Guajardo, Bosche

Complementary IBS: Application Specific Error Correction for PUFs
Matthias Hiller, Dominik Merli, Frederic Stumpf and Georg Sigl (Technical University of Munich)

Buskeeper PUFs, a Promising Alternative to D Flip-Flop PUFs
Peter Simons, Erik van der Sluis and Vincent van der Leest (Intrinsic-ID)

Bit Stream Analysis of Physical Unclonable Functions based on Resistance Variations in Metals and Transistors
Jing Ju, Raj Chakraborty, Reza Rad and Jim Plusquellic (University of New Mexico)

11:45 - 1:00: Lunch

1:00 - 2:00: Poster Session
Session Chair: Ted Huffmire, Naval Postgraduate School

A Novel Method for Watermarking Sequential Circuits
Matthew Lewandowski, Richard Meana, Srinivas Katkoori and Matthew Morrison (University of South Florida)

Reliability Enhancement of Bi-Stable PUFs in 65nm Bulk CMOS
Mudit Bhargava, Cagla Cakir and Ken Mai (Carnegie Mellon University)

SDMLp: On the Use of Complementary Pass Transistors for Design of DPA Resistant Circuits
Manoj Chakkaravarthy, Lakshmi Narasimhan Ramakrishnan, Antarpreet Singh Manchanda, Mike Borowczak and Ranga Vemuri (University of Cincinnati)

Register Leakage Masking Using Gray Code
Houssem Maghrebi, Emmanuel Prouff, Sylvain Guilley and Jean-Luc Danger (ENST, France)

An Adaptable, Modular, and Autonomous Side-Channel Vulnerability Evaluator
Michael Zohner, Marc Stöttinger, Sorin A. Huss and Oliver Stein (CASED, TU Darmstadt)

Evaluating Security Requirements in a General-Purpose Processor by Combining Assertion Checkers with Code Coverage
Michael Bilzor, Ted Huffmire, Cynthia Irvine and Tim Levin (Naval Postgraduate School)

HTOutlier: Hardware Trojan Detection with Side-Channel Signature Outlier Identification
Jie Zhang, Haile Yu and Qiang Xu (Chinese University of HongKong)

FPGA based Trustworthy Authentication Technique using Physically Unclonable Functions and Artificial Intelligence
Swetha Pappala, Mohammed Niamat and Weiqing Sun (University of Toledo)

t-private Logic Synthesis on FPGA
Jungmin Park and Akhilesh Tyagi (Iowa State University)

2:00 - 2:20: Break

2:20 - 3:35: Hardware Trojans
Session Chair: Ingrid Verbauwhede, KU Leuven

Interacting with Hardware Trojans Over a Network
Mohammed Farag, Lee Lerner and Cameron Patterson (Virginia Tech)

Trojan Detection based on Delay Variations Measured using a High-Precision, Low-Overhead Embedded Test Structure
Charles Lamech and Jim Plusquellic (University of New Mexico)

Reverse Engineering Circuits Using Behavioral Pattern Mining
Wenchao Li, Zach Wasson and Sanjit Seshia (University of California, Berkeley)

3:35 - 4:00: Break

4:00 -5:15: Countermeasures I
Session Chair: William Robinson, Vanderbilt

Glitch-Free Implementation of Masking in Modern FPGAs
Amir Moradi and Oliver Mischke (Horst Görtz Institute for IT-Security, Ruhr University Bochum)

A Systematic M safe-error Detection in Hardware Implementations of Cryptographic Algorithms
Dusko Karaklajic, Junfeng Fan and Ingrid Verbauwhede (KU Leuven)

Functional Integrated Circuit Analysis
Dmitry Nedospasov, Alexander Schloesser, Susanna Orlic and Jean-Pierre Seifert (TU Berlin)

5:15 - 6:00: Reception & Best Paper Award

Monday – June 4, 2012

9:00 - 10:00: Industrial Session
Session Chair: Jim Plusquellic, University of New Mexico

Performance Metrics and Empirical Results of a PUF Cryptographic Key Generation ASIC
Meng-Day Yu, Richard Sowell, Alok Singh, David M'Raihi (Verayo) and Srinivas Devadas (MIT)

HSDL: A Security Development Lifecycle for Hardware Technologies
Hareesh Khattri, Narasimha Kumar V Mangipudi and Salvador Mandujano (Intel)

10:00- 10:20: Break

10:20 - 11:35: Countermeasures II
Session Chair: Jean-Luc Danger, Telecom ParisTech

Design Solutions for Securing SRAM Cell Against Power Analysis
Vladimir Rozic, Wim Dehaene and Ingrid Verbauwhede (KU Leuven)

On Charge Sensors for FIB Attack Detection
Clemens Helfmeier, Christian Boit and Uwe Kerst (TU Berlin)

Detection of Probing Attempts in Secure ICs
Salvador Manich, Markus S. Wamser and Georg Sigl (TU Darmstadt)

11:45 - 1:00: Lunch

1:00 – 2:30: Dangers of Counterfeit Electronic Components: Detection Challenges, Solutions and Policies
Moderator: Mohammad Tehranipoor, U. Connecticut

Panelists:

Tom Sharpe, SMT Corp.

Saverio Fazzari, Booz Allen Hamilton

Ben Epstein, OpCoast

Diganta Das, University of Maryland

Philip Comer, DMEA

Mark Marshall, Integra Technologies

2:30 - 2:50: Break

2:50 - 3:40: Side-channel Attacks and Fault Attacks
Session Chair: Saverio Fazzari, Booz Allen Hamilton

Fault Round Modification Analysis of the Advanced Encryption Standard
Jean-Max Dutertre, Amir-Pasha Mirbaha, Naccache David, Anne-Lise Ribotta, Assia Tria and Thierry Vaschalde (EMSE France, ENS Paris, CEA-LETI)

Improved Algebraic Side Channel Attack on AES
Mohamed Saied Emam Mohamed, Stanislav Bulygin, Zohner Michael, Walter Michael and Heuser Annelie (TU Darmstadt)

3:40 - 4:00: Closing remarks