



June 5-6, 2011
San Diego Convention Center
San Diego, CA

IEEE Sponsors

IEEE
SECURITY & PRIVACY

tttc

IEEE
computer
society

Industry Sponsors



Sunday 5 June 2011

8:40 - 9:00: Opening Remarks

Ken Mai (CMU) and Patrick Schaumont (Virginia Tech)

9:00 - 10:00: Keynote Speech

Session Chair: Ken Mai

Security Challenges and Opportunities in Adaptive and Reconfigurable Hardware

Srinivas Devadas (MIT)

10:00 - 10:20: Break

10:20 - 11:35: IP Protection and Trojan Detection

Session Chair: Ramesh Karri

TinyTPM: A Lightweight Module aimed to IP Protection and Trusted Embedded Platforms

Thomas Feller, Sunil Malipatlolla, David Meister and Sorin A. Huss (CASED)

Enhancing Security via Provably Trustworthy Hardware Intellectual Property

Eric Love, Yier Jin and Yiorgos Makris (Yale University)

ODETTE: A Non-Scan Design-for-Test Methodology for Trojan Detection in ICs

M. Banga and M. Hsiao (Virginia Tech)

11:45 - 1:00: Lunch

1:00 - 2:00: Poster Session

Session Chair: Patrick Schaumont

Influence of the Temperature on True Random Number Generators

Mathilde Soucarros, Cécile Canovas-Dumas, Jessy Clédière, Philippe Elbaz-Vincent and Denis Réal (CEA-LETI, Institut Fourier, DGA-MI)

Implementation and Verification of DPA-Resistant Cryptographic DES Circuit using Domino-RSL

Katsuhiko Iwai, Mitsuru Shiozaki, Anh-Tuan Hoang, Kenji Kojima and Takeshi Fujino (Ritsumeikan University)

Security Checkers: Detecting Processor Malicious Inclusions at Runtime

Michael Bilzor, Ted Huffmire, Cynthia Irvine and Tim Levin (Naval Postgraduate School)

Formal Security Evaluation of Hardware Boolean Masking against Second-Order Attacks

Housseem Maghrebi, Sylvain Guilley and Jean-Luc Danger (CNRS/LTCI)

TrustGeM: Dynamic Trusted Environment Generation for Chip-Multiprocessors

Luis Bathen and Nikil Dutt (UC Irvine)

Performance Evaluation of Protocols Resilient to Physical Attacks

Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Nidhal Selmane and Denis Real (CNRS/LTCI, DGA-MI)

Flexible Architecture Optimization and ASIC Implementation of Group Signature Algorithm using a Customized HLS Methodology

Sumio Morioka, Toshiyuki Isshiki, Satoshi Obana, Yuichi Nakamura and Kazue Sako (NEC)

High Level Security Evaluation Method Against Safe-error Attacks

Dusko Karaklajic, Junfeng Fan and Ingrid Verbauwhede (KU Leuven)

Case Study: Detecting Hardware Trojans in Third-Party Digital IP Cores

Xuehui Zhang and Mohammad Tehranipoor (University of Connecticut)

TeSR: A Robust Temporal Self-Referencing Approach for Hardware Trojan Detection

Seetharam Narasimhan, Xinmu Wang, Dongdong Du, Rajat Subhra Chakraborty and Swarup Bhunia (Case Western Reserve University)

2:00 - 2:20: Break

2:20 - 3:35: Methods for Side-channel Analysis

Session Chair: Kazuo Sakiyama

Algorithmic Collision Analysis for Evaluating Cryptographic Systems and Side-channel Attacks

Qiasi Luo and Yungsi Fei (University of Connecticut)

Accelerating Early Design Phase Differential Power Analysis Using Power Emulation Techniques

Armin Krieg, Christian Bachmann, Johannes Grinschgl, Christian Steger, Reinhold Weiss and Josef Haid (TU Graz)

A Fast Power Current Analysis Methodology using Capacitor Charging Model for Side Channel Attack Evaluation

Daisuke Fujimoto, Makoto Nagata, Toshihiro Katashita, Akihiko Sasaki, Yohei Hori and Akashi Satoh (Kobe University, AIST)

3:35 - 4:00: Break**4:00 -5:15: Secure Architecture**

Session Chair: Divya Arora

Hardware Security in Practice: Challenges and Opportunities
Nachiketh Potlapally (Intel)

Low-cost recovery for the code integrity protection in secure embedded processors

Minh Huu Nguyen, Bruno Robisson, Michel Agoyan and Nathalie Drach (CEA Leti)

New security threats against chips containing scan chain structures

Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes and Bruno Rouzeyre (LIRMM)

5:15 - 6:00: Reception & Best Paper Award**Monday 6 June 2011****8:30 - 9:45: Industrial Session**

Session Chair: Jim Plusquellic

Placement of Trust Anchors in Embedded Computer Systems
Steve Papa, William D Casper and Suku Nair (Lockheed Martin and Southern Methodist University)

MARVEL - Malicious Alteration Recognition and Verification by Emission of Light

Peilin Song (IBM)

A Survey of Frequently Identified Vulnerabilities in Commercial Computing Semiconductors

Kevin Gotze (Intel)

9:45 - 10:15: Break**10:15 - 12:00: Physical Unclonable Functions**

Session Chair: Farinaz Koushanfar

Invited: Hardware Intrinsic Security based on SRAM PUFs: Tales from the Industry

Helena Handschuh (Intrinsic-ID)

Reliable and Efficient PUF Key Generation Using Pattern Matching

Srini Devadas and Zdenek Paral (MIT)

The Bistable Ring PUF: A New Architecture for Strong Physical Unclonable Functions

Qingqing Chen, Gyorgy Csaba, Paolo Lugli, Ulf Schlichtmann and Ulrich Rührmair (TU Munich)

On Improving Reliability of Delay Based Physically Unclonable Functions under Temperature Variations

Raghavan Kumar, Harikrishnan Kumarapillai Chandrikakutty and Sandip Kundu (University of Massachusetts at Amherst)

12:00 - 1:30: Lunch**1:30 - 3:00: Panel: Can I Hack Your Brain?**

Moderator: Ingrid Verbauwhede, KU Leuven

Panelists: J. Rabaey (UC Berkeley)

K. Fu (UMass Amherst)

R. Rajagopalan (HP Labs)

3:00 - 3:20: Break**3:20 - 4:35: Side-channel Attacks and Fault Attacks**

Session Chair: Francesco Regazzoni

Revisit Fault Sensitivity Analysis on WDDL-AES

Yang Li, Kazuo Ohta and Kazuo Sakiyama (University of Electro Communications)

Practical Evaluations of DPA Countermeasures on Reconfigurable Hardware

Amir Moradi, Oliver Mischke and Christof Paar (University of Bochum)

A Novel Fault Attack Against ECDSA

Alessandro Barenghi, Guido Bertoni, Andrea Palomba and Ruggero Susella (Politecnico di Milano and ST Microelectronics)

4:35 - 4:45**Closing remarks**