HOST 2016 Preliminary Program

May 3-5, 2016
McLean, VA, USA
The Ritz-Carlton, Tysons Corner
Salon 3, 5th Floor

FEATURED SPEAKERS

Keynote Talk
Donna F. Dodson
NIST

Keynote Talk
Allan Steinhardt
Booz Allen Hamilton

Keynote Talk
Frank McKeen
Security Research Lab, Intel

Keynote Talk
Carl E. McCants
IARPA

Visionary Talk
Kerry Bernstein
DARPA

Visionary Talk
Apostol Vassilev
NIST

Visionary Talk
Lok Yan
Air Force Research Lab

Invited Industry Talk
Brian Murray
ZF-TRW

Invited Industry Talk
Mark E. Marson
Cryptography Research, Inc.

Invited Industry Talk
Michael Schuldenfrei
Optimal+

HOST 2016 Program Highlights

- **10 Featured Invited Speakers showcasing some of the world's most innovative thinkers in hardware security! It includes 4 Keynote Talks, 3 Visionary Talks and 3 invited industry talks.**
- **26 Technical Paper and 18 Poster Presentations**
- **Two Panels on topics of emerging importance**
- **"Hardware Demo Competition" – first time in HOST 2016**
- **Industry Exhibit Tables – first time in HOST 2016**
- **Reception and Award Presentation on the second day**
- **Lunch Plenary Talks and more**

Tuesday, May 3 | Salon 3, 5th Floor

7:30 – 8:30am Registration and Continental Breakfast

SESSION 1: PLENARY SESSION
Moderator: Swarup Bhunia, University of Florida

8:30 – 8:45am Opening Remarks: HOST 2016 General and Program Chairs

8:45 – 9:30am KEYNOTE I
Session Chair: William H Robinson, Vanderbilt University

Speaker: Donna F. Dodson, Chief Cybersecurity Advisor and ITL Associate Director for Cybersecurity, National Institute of Standards and Technology (NIST)
Title: *Building Trust from the Bottom Up – A NIST perspective*

9:30 – 10:00am INVITED VISIONARY TALK
Session Chair: Ankur Srivastava, University of Maryland

Speaker: Kerry Bernstein, Defense Advanced Research Projects Agency (DARPA)
Title: *Gazing into the Hardware Security Crystal Ball*

10:00 – 10:30am BREAK

10:30 – 12:10pm SESSION 2: HARDWARE AUTHENTICATION & PUF
Session Chair: Arun Kanuparthi, Intel, USA

- *Robust Privacy-preserving Fingerprint Authentication*[**]
  Ye Zhang and **Farinaz Koushanfar** – Rice U., TX, USA

- *UCR: Unclonable Chipless RFID Tag*[**]
  Kun Yang, **Domenic Forte** and **Mark Tehranipoor** – U. of Florida, FL, USA

- *A Highly Reliable and Tamper-Resistant RRAM PUF: Design and Experimental Validation*
  Rui Liu – Arizona State U., AZ, USA
  Huaqiang Wu, Yachuan Pang, He Qian – Tsinghua U., Beijing, China
  Shimeng Yu – Arizona State U., AZ, USA

- *Machine Learning Resistant Strong PUF: Possible or a Pipe Dream?*
  Arunkumar Vijayakumar, **Vinay C Patil** – U. of Massachusetts Amherst, MA, USA
  Charles B. Prado – National Institute of Metrology, Quality and Technology, Brazil
  Sandip Kundu – U. of Massachusetts Amherst, MA, USA

- *LEDPUF: Stability-Guaranteed Physical Unclonable Functions through Locally Enhanced Defectivity*
  Wei-Che Wang, **Yair Yona**, **Suhas Diggavi**, and **Puneet Gupta** – U. of California, LA, USA

12:10 – 1:30pm LUNCH

12:30 – 1:10pm Lunch Talk
Speaker: Pim Tuyls, Founder and CEO, Intrinsic ID
Session Chair: Jeyavijayan (JV) Rajendran, The University of Texas at Dallas
Title: *Because Failure is not an Option: Physical Unclonable Functions*

1:30 – 3:10pm SESSION 3: EFFICIENT IMPLEMENTATION OF SECURE SYSTEMS
Session Chair: Shimeng Yu, Arizona State University

- *Parsimonious Design Strategy for Linear Layers with High Diffusion in Block Ciphers*
  Sikhar Patranabis, Debapriya Basu Roy, Yash Shrivastava, Debdeep Mukhopadhyay – IIT Kharagpur, India
  Santosh Ghosh – Intel labs, Oregon, USA

- *Iterating Von Neumann's Post-Processing under Hardware Constraints*
  Vladimir Rozic, Bohan Yang, Wim Dehaene and **Ingrid Verbauwhede** – KU Leuven, Belgium

- *Controlling your Control Flow Graph*
  Arun Kanuparthi – Intel Corporation, USA
  Jeyavijayan Rajendran – U. of Texas at Dallas, TX, USA
  Ramesh Karri – New York U., NY, USA

- *An Area Optimized Serial Implementation of ICEPOLE Authenticated Encryption Scheme*
  Michael Tempelmeier, Fabrizio De Santis – Technische Universität München, Germany
  Jens-Peter Kaps – George Mason U., VA, USA
  Georg Sigl – Technische Universität München, Germany

- *Round Gating for Low Energy Block Ciphers*
  Subhadeep Banik, Andrey Bogdanov – Technical University of Denmark, Denmark
  Francesco Regazzoni – dvanced Learning and Research Institute, Switzerland
  Takanori Isobe, Toru Akishita and **Harunaga Hiwatari** – Sony Corporation, Japan

3:10 – 3:40pm AFTERNOON KEYNOTE
Session Chair: Yier Jin, University of Central Florida
Speaker: Frank McKeen, Security Research Lab, Intel, USA
Title: *Protecting Enterprise Data while in Use*

3:40 – 5:00pm BREAK and SESSION 4: POSTER SESSION
Session Chair: Qiaoyan Yu, University of New Hampshire

Poster session starts with 1-minute oral presentation for each poster.

See below for the list of poster presentations

5:00 – 6:15pm SESSION 5: INVITED INDUSTRY SESSION: New Directions in Hardware Security
Session Chair: Yousef Iskander, Cisco

Speakers:

1. **Michael Schuldenfrei**, Chief Technology Officer, Optimal+
   Title: *Enabling Supply Chain Security Assurance through an Authentication Data Network*

2. **Brian Murray**, Director, Safety and Security Excellence, Zf TRW
   Title: *Hardware-Assisted Cyber Security in Automotive Systems*

3. **Mark Marson**, Technical Director, Cryptography Research
   Title: *Efficient and Cost-Effective Testing for Side Channel Vulnerabilities*

Wednesday, May 4 | Salon 3, 5th Floor

7:45 – 8:45am Registration and Continental Breakfast

SESSION 6: PLENARY SESSION
Moderator: Swarup Bhunia, University of Florida

8:45 – 9:30am KEYNOTE III
Session Chair: Saverio Fazzari, Booz Allen Hamilton

Speaker: Allan Steinhardt, Fellow and Senior Executive Advisor, Booz Allen Hamilton
Title: *"Technical Means to Detect Counterfeiting in the Real World: What the Government is Thinking, and How it is Driving Industry"*

9:30 – 10:00am INVITED VISIONARY TALK
Session Chair: Domenic Forte, University of Florida

Speaker: Lok Yan, Air Force Research Lab, USA
Title: *HOST: HOST Oriented Security and Trust*

10:00 – 11:00am BREAK and SESSION 7: HARDWARE DEMO COMPETITION

Hardware Demo Chair: Jim Plusquellic, University of New Mexico

See below for the list of hardware demos

11:00 – 12:00pm SESSION 8: ATTACKS & FORENSICS
Session Chair: Wujie Wen, Florida International University

- *A Layout-driven Framework to Assess Vulnerability of ICs to Microprobing Attacks***
  Qihang Shi – U. of Connecticut, CT, USA
  Navid Asadizanjani, Domenic Forte and **Mark Tehranipoor** – U. of Florida, FL, USA

- *A New Approach for Rowhammer Attacks*
  Rui Qiao – Stony Brook U., NY, USA
  Mark Seaborn – Google, USA

- *Hardware-based Workload Forensics: Process Reconstruction via TLB Monitoring*
  Liwei Zhou and **Yiorgos Makris** – The U. of Texas at Dallas, TX, USA

12:00 – 1:20pm LUNCH

12:30 – 1:00pm Lunch Talk

Speaker: Jim Plusquellic, CTO, Charles E. Mendez Jr., CEO, Enthentica
Session Chair: Ryan Helinski, Sandia National Labs, USA

Title: *Strong PUF-based Authentication for IoT and Beyond*

1:20 – 3:00pm SESSION 9: SYSTEM SECURITY: RISK ANALYSIS & SOLUTIONS
Session Chair: Ioannis Savidis, Drexel University

- *A Key-centric Processor Architecture for Secure Computing***
  David Whelihan, Kate Thurmer and **M. Michael Vai** – MIT Lincoln Laboratory, MA, USA

- *Hardware Security Risk Assessment: A Case Study*
  Brent Sherman and **David Wheeler** – Intel Corporation, USA

- *A Novel Security Technique for Generating Truly Random and Reliable Reconfigurable ROPUF-Based Cryptographic Keys*
  Fathi Amsaad, Atul Prasad Deb Nath and **Mohamed Niamat** – The U. of Toledo, OH, USA

- *A Zero-cost Approach to Detect Recycled SoCs Using Embedded SRAM*
  Zimu Guo, Md. Tauhidur Rahman, Mark Tehranipoor and **Domenic Forte** – U. of Florida, FL, USA

- *Redirecting DRAM Memory Pages: Examining the Threat of System Memory Hardware Trojans*
  Bradley Hopkins, John Shield and **Chris North** – Australia Department of Defense, Australia

3:00 – 3:20pm BREAK

3:20 – 4:20pm SESSION 10: SIDE CHANNELS: THE GOOD AND THE BAD
Session Chair: Fareena Saqib, Florida Institute of Technology

- *Large Laser Spots and Fault Sensitivity Analysis***
  Falk Schellenberg, Markus Finkeldey, Nils Gerhardt, Martin Hofmann, Amir Moradi and **Christof Paar** – Ruhr-U. Bochum, Germany

- *The Other Side of the Coin: Analyzing Software Encoding Schemes against Fault Injection Attacks*
  Jakub Breier, Dirmanto Jap and **Shivam Bhasin** – Nanyang Technological U., Singapore

- *IP Core Protection using Voltage-Controlled Side-Channel Receivers*
  Peter Samarin, Kerstin Lemke-Rust – Bonn-Rhein-Sieg U. of Applied Sciences, Germany
  Christof Paar – Ruhr-U. Bochum, Germany

4:20 – 5:50pm SESSION 11: PANEL I

Topic: *Hardware-enabled System Security*

Panel Moderator: Saverio Fazzari, Booz Allen Hamilton

Panelists:

- Tony Jeffs, Cisco Systems
- Tom Tkacik, NXP Semiconductor
- Jim Fahrny, Comcast
- Ethan Cannon, Boeing
- Serge Leef, Mentor Graphics

6:00pm RECEPTION and AWARD ANNOUNCEMENTS

Thursday, May 5 | Salon 3, 5th Floor

7:45 – 8:45am Continental Breakfast

SESSION 12: PLENARY SESSION
Moderator: Ryan Kastner, University of California, San Diego

8:45 – 9:30am KEYNOTE IV
Session Chair: Gang Qu, University of Maryland

Speaker: Carl E. McCants, Intelligence Advanced Research Projects Activity (IARPA)
Title: *From Star Trek to Star Wars: The Force Awakens - The Importance of Hardware and IP Security*

9:30 – 10am: **INVITED VISIONARY TALK**
Session Chair: Greg Creech, Electroscience Lab, USA

Speaker: Apostol Vassilev, Technical Director, National Institute of Standards and Technology (NIST)
Title: *Cybersecurity Today and Tomorrow: Assurance or Insurance?*

10:00 – 10:30am BREAK

10:30 – 12:10pm SESSION 13: ATTACK-RESISTANT DESIGN and PROTOCOLS
Session Chair: Aaron E. Cohen, NRL, Washington, DC

- *A Separation and Protection Scheme for On-chip Memory Blocks in FPGAs*
  Luis Ramirez Rivera, **Xiaofang Wang** and **Danai Chasaki** – Villanova U., PA, USA

- *A Secure Camouflaged Threshold Voltage Defined Logic Family*
  Burak Erbagci – Carnegie Mellon U., PA, USA
  Cagri Erbagci – Sabanci U., Turkey
  Nail Etkin, **Can Akkaya** and **Ken Mai** – Carnegie Mellon U., PA, USA

- *SARLock: SAT Attack Resistant Logic Locking*
  Muhammad Yasin – New York U., NY, USA
  Bodhisatwa Mazumdar – New York U. Abu Dhabi, United Arab Emirates
  Jeyavijayan Rajendran – U. of Texas at Dallas, TX, USA
  Ozgur Sinanoglu – New York U. Abu Dhabi, United Arab Emirates

- *Classification Algorithms for Template Matching*
  Elif Ozgen– Technische Universiteit Eindhoven, Netherlands
  Louiza Papachristodoulou and **Lejla Batina** – Radboud University Nijmegen, Netherlands

- *GenMatch: Secure DNA Compatibility Testing*
  M. Sadegh Riazi, Neeraj Kumar Reddy Dantu, Laxmi Narasima Vinay Gattu and **Farinaz Koushanfar** – Rice U., TX, USA

12:10 – 1:10pm LUNCH

1:10 – 2:50pm SESSION 14: PANEL II
Topic: *Hardware IP Protection through Invasive and Non-invasive Analysis*
Panel Moderator: Mark Tehranipoor, University of Florida

Panelists:

- Edward Principe, Tescan USA Inc.
- Yier Jin, University of Central Florida
- Chris Pawlowicz, TechInsights
- Len Orlando, Air Force Research Lab
- Steve Trimberger, Xilinx
- Matthew Scholl, NIST

2:50 – 3:00pm pm CONCLUDING REMARKS

HOST 2016 and HOST 2017 General and Program Chairs

*** HOST 2016 Best paper Nominee*

POSTERS:

- *Functional Polymorphism for Intellectual Property Protection*
  Jeffrey McDonald – U. of South Alabama, AL, USA
  Yong Kim – Air Force Research Lab, USA
  Todd Andel – U. of South Alabama, AL, USA
  James McVicar – TruBridge, USA
  Miles Forbes – U. of South Alabama, AL, USA

- *The Conjoined Microprocessor*
  Ehsan Aerabi – Iran U. of Science and Technology, Iran
  A.Elhadi Amirouche – Sorbonne Universités – Université Paris II, France
  Houda Ferradi, Sha Rémi Geraud, Naccache David and **Jean Vuillemain** – Ecole normale suprieure, France

- *Low-Area Hardware Implementations of CLOC, SILC and AES-OTR*
  Subhadeep Banik, Andrey Bogdanov – Technical U.of Denmark, Denmark
  Kazuhiko Minematsu – NEC Corporation, Japan

- *Functional Block Identification in Circuit Design Recovery*
  Jacob Couch, Elizabeth Reilly, Morgan Schuyler and **Brad Barrett** – Johns Hopkins U., MD, USA

- *Robust Hardware True Random Number Generators using DRAM Remanence Effects*
  Fatemeh Tehranipoor, Wei Yan and **John Chandy** – U. of Connecticut, CT, USA

- *Blinded random corruption attacks*
  Shay Gueron – U. of Haifa, Israel
  Rodrigo Branco – Intel Corporation, USA

- *Trust Games: How Game Theory Can Guide the Development of Hardware Trojan Detection Methods*
  Jonathan Graf – Graf Research, USA

- *ACBuilder: A Tool for Hardware Architecture Security Evaluation*
  Henrique Kawakami, Ricardo Dahab, Roberto Gallo – Unicamp, Brazil
  David Ott and **Hao-Chi Wong** – Intel Corporation, USA

- *On the Problems of Realizing Reliable and Efficient Ring Oscillator PUFs on FPGAs*
  Alexander Wild, Georg T. Becker – Ruhr-U. Bochum, Germany
  Tim Güneysu – U. of Bremen & DFKI, Germany

- *Model Checking to Find Vulnerabilities in an Instruction Set Architecture*
  Chris Bradfield – Weebly Inc., USA
  Cynthia Sturton – U. of North Carolina at Chapel Hill, NC, USA

- *Scalable and privacy-preserving outsourcing of learning algorithms*
  Azalia Mirhoseini, Farinaz Koushanfar – Rice U., TX, USA
  Ahmad-Reza Sadeghi – Technische Universität Darmstadt, Germany

- *Fast and Scalable Security Support for Directory-Based Distributed Shared Memory*
  Ofir Shwartz and **Yitzhak Birk** – Technion, Israel

- *Adaptive Real-time Trojan Detection Framework through Machine Learning*
  Amey Kulkarni – U. of Maryland Baltimore County, MD, USA
  Youngok Pino – Naval Sea Systems Command, USA
  Tinoosh Mohsenin – U. of Maryland Baltimore County, MD, USA

- *Scalable SoC Trust Verification using Integrated Theorem Proving and Model Checking*
  Xiaolong Guo, Raj Gautam Dutta – U. of Central Florida, FL, USA
  Prabhat Mishra – U. of Florida, FL, USA
  Yier Jin – U. of, Central Florida, FL, USA

- *Information Leakage behind the Curtain: Abusing Anti-EMI Features for Covert Communication*
  Johannes Bauer – Friedrich-Alexander Universität Erlangen-Nürnberg, Germany
  Sebastian Schinzel – Münster University of Applied Sciences, Germany
  Felix Freiling – Friedrich-Alexander Universität Erlangen-Nürnberg, Germany
  Andreas Dewald – ERNW Research GmbH, Heidelberg, Germany

- *Granularity and detection capability of an adaptive embedded Hardware Trojan detection system*
  Maxime Lecomte, Jacques Fournier – CEA Tech, France
  Philippe Maurine – LIRMM, France

- *Electronic Forensic Techniques for Manufacturer Attribution*
  Ryan Helinski, Ed Cole, Gideon Robertson, Jonathan Woodbridge, Lyndon Pierson – Sandia National Laboratories, USA

- *Integrated All-Digital Low-dropout Regulator as a Countermeasure to Power Attack in Encryption Engines*
  Arvind Singh, Monodeep Kar, Saibal Mukhopadhyay – Georgia Tech, GA, USA
  Anand Rajan and Vivek De – Intel Labs, OR, USA

HARDWARE DEMOS:

- *Design Security Rule Check: Vulnerability Analysis for DFT Exploits of SoCs*
  Gustavo K. Contreras, **Adib Nahiyan**, **Domenic Forte**, and **Mark Tehranipoor** – U. of Florida, FL, USA
  A major challenge with designing secure Systems -on-Chip (SoCs) is the diversity of existing and emerging attacks and potential countermeasures. A framework, called Design Security Rule Check (DSeRC), can be integrated in the conventional SoC design flow to analyze vulnerabilities of a design and assess its security at various stages of the design process, namely register transfer level (RTL), gate-level netlist, design-for-test (DFT) insertion, physical design, etc. The demonstration will show the automated vulnerability analysis tool in real-time.

- *A Strong-PUF Authentication Protocol for Resource-Constrained Devices*
  Wenjie Che and **Jim Plusquellic** – U. of New Mexico, NM, USA
  The SHA-3 (keccakf200) secure hash algorithm is implemented on a Xilinx Zynq FPGA as a mechanism to implement a PUF-based authentication protocol. A hardware-embedded delay PUF called HELP integrates into the SHA-3 implementation to enable dual use of the functional unit, i.e., as a secure hash function and as a source of entropy for bitstrings used in the authentication protocol. A full client-server based authentication protocol, including enrollment, will be demonstrated between a set of FPGAs (tokens) and a secure server (a laptop).

- *A Low-Cost Portable Spectroscopic Device for Authentication of Medicines and Food Products*
  Cheng Chen – Case Western Reserve U., OH, USA
  Fengchao Zhang – U. of Florida, FL, USA
  Soumyajit Mandal – Case Western Reserve U., OH, USA
  A chemometric passport approach is demonstrated for authenticating pharmaceutical supply chain medicines as a means of providing quality assurance and addressing public health issues.

- *ReSC: An RFID-Enabled Solution for Defending IoT Supply Chain*
  Kun Yang, Domenic Forte and **Mark M. Tehranipoor** – U. of Florida, FL, USA
  An RFID-enabled technique is demonstrated that aims at defending the IoT supply chain by addressing two major issues including the disappearance/theft of authentic IoT devices and appearance of counterfeit IoT devices.

- *Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Evaluation*
  Yu Liu and **Yiorgos Markis** – The U. of Texas at Dallas, TX, USA
  The threat of hardware Trojans in wireless cryptographic ICs, as well as the effectiveness of two detection methods, is demonstrated using a custom-designed chip consisting of an Advanced Encryption Standard (AES) core and an Ultra-Wide-Band (UWB) transmitter.

- *Firmware Instruction Identification Using Side-Channel Power Analysis*
  Chintan Patel and **Ryan Robucci** – U. of Maryland, Baltimore County, MD, USA
  A side-channel analysis is performed over multiple power supply pins to demonstrate the relationship between the power transients and machine-level instructions on an instance of the openMSP430 processor on an FPGA.

- *Configurable Ring Oscillator PUF as an Entropy Pump*
  Qian Wang and **Gang Qu** – U. of Maryland, MD, USA
  A silicon physical unclonable function (PUF) is used as an entropy source to enhance a random input string. This is accomplished by using an input random string as the configuration vector for the flexible ring oscillator (RO) PUF which generates another random string (the PUF bits).

- *Multi-Communication Type Debugging Probe*
  Austin Funes, Cheng Guo, Somtochukwu Okwuosah, Fatemeh Tehranipoor and **John Chandy** – U. of Connecticut, CT, USA
  A Multi-Communication Type Debugging (MCTD) probe is demonstrated, which is capable of identifying the test pins on a PCB and for auto-detecting the communication protocol being used by the device with only a small amount of information available to the user.

- *Robotic Arm based CPS Security Platform*
  Kelvin Ly and **Yier Jin** – U. of Central Florida, FL, USA
  A robotic arm system is demonstrated that can be used as a testbed for CPS security and the related fields in robust and cooperative control systems. The arms are connected together in a wireless network, allowing for remote programming and message passing between the arms themselves. Some simple tasks are demonstrated to allow performance to be benchmarked.

- *Potential Pitfall of RLUT: Fault Attack using Hardware Trojan*
  Debapriya Basu Roy, Shivam Bhasin, Sikhar Patranabis, Sylvain Guilley, Jean-Luc Danger, Debdeep Mukhopadhyay, Xuan Thuy Ngo and **Zakaria Najm** – Telecom ParisTech, Paris, France
  Dynamic reconfiguration via a look-up table (RLUT) in modern FPGAs allows users to modify the functionality of LUTs at runtime. This hardware demonstration shows a stealthy hardware Trojan in an untrusted IP vendor attack scenario.

- *Quantified Analysis of Magnetic Attack on Commercial Magnetic RAM Chip*
  Alexander Holst and **Swaroop Ghosh** – U. of South Florida, FL, USA
  Magnetoresistive random-access memory (MRAM) is a prime candidate to become a universal memory to serve all requirements for information storage, from short-term to long-term. This demonstration will show the vulnerability of MRAM to externally-applied static magnetic fields by correlating the magnetic field strength with the gross error rate observed on a commercial MRAM chip.

- *Prototype Demonstration of Secure Control Area Network (CAN) against Masquerade and Replay Attacks*
  Mohammad Raashid Ansari, Qiaoyan Yu and **Tom Miller** – U. of New Hampshire, NH, USA
  CAN is one of the widely used communication buses in an automobile to connect electronic control units (ECUs). The design of the CAN protocol renders it defenseless against emerging masquerade and replay attacks. This hardware demonstration investigates hardware/firmware-level methods to detect and mitigate these types of attacks.

- *Charging Battery for Information Leakage*
  Khoa Hoang, Jacob Wurm and **Yier Jin** – U. of Central Florida, FL, USA
  A charging battery of an iPhone or Android phone is modified in this hardware demonstration to include malicious components that can control the smart phone to do anything such as making phone calls, download apps, etc.

- *Demonstration of a Hardware Trojan Attack in an IEEE 802.11a/g Network*
  Kiruba S. Subramani, Angelos Antonopoulos, Aria Nosratinia, and **Yiorgos Makris** – The U. of Texas at Dallas, TX, USA
  Wireless networks are now prevalent in sensor applications and the Internet of Things. Even though wireless devices use some form of encryption, the underlying hardware is still vulnerable to hardware Trojans. This hardware demonstration (i) describes the risks posed by hardware Trojans in wireless networks (ii) elucidate the risk by developing realistic attacks (iii) demonstrate attacks on experimental platforms and (iv) develop defense mechanisms.

- *Flexible, Opensource workbench for Side-channel analysis (FOBOS)*
  Rajesh Velegalati, Panasayya Yalla and **Jens-Peter Kaps** – George Mason U., VA, USA
  Side-channel analysis attacks pose a grave threat to implementations of cryptographic algorithms implemented in software as well as in hardware. The demonstrated FOBOS technique simplifies the task of carrying out side-channel attacks by supporting multiple FPGA devices, and including all necessary software to run differential power analysis attacks, which are the most prominent kind of side-channel attacks.

Corporate Sponsors

PLATINUM

INTRINSIC ID

GOLD

ENTHENTICA

intel

Rambus
Cryptography Research

SILVER

cisco

Mentor Graphics

Microsemi

Tortuga Logic

Student Travel Grant Sponsors

NSF

Organizational Sponsors

TRUST

IEEE computer society