

AsianHOST 2016 Preliminary Program

AsianHOST 2016 Program Highlights

- 5 Featured Invited Speakers showcasing some of the world's leading innovative thinkers in hardware security! It includes 2 Keynote Talks, 4 Invited Talks.
- 24 Technical Papers
- One panel on industrial view towards hardware security
- One sponsored industrial talk
- Student poster session
- The first international hardware security forum in Asia

Monday, December 19, 2016

7:15 – 8:15AM Registration

SESSION 1: PLENARY SESSION

Moderator: Gang Qu, University of Maryland

8:15 – 8:30AM Welcome Remarks: AsianHOST 2016 General and Program Chairs

8:30 – 9:15AM KEYNOTE I

Speaker: Tim Cheng, Dean of Engineering, Hong Kong University of Science and Technology

Title: *Security Threats in Hardware Design's Unspecified Functionality*

9:15 – 9:50AM INVITED TALK

Speaker: Tsutomu Matsumoto, Yokohama National University

Title: *Nano Artifact Metrics Using Silicon Random Nanostructures*

9:50 – 10:20AM BREAK

10:20 – 12:00PM SESSION 2: PUF DESIGN AND APPLICATIONS

Session Chair: Qiaoyan Yu, University of New Hampshire

- *Upper Bounds on The Min-Entropy of RO Sum, Arbiter, Feed-Forward Arbiter, and S-ArbRO PUFs*
Jeroen Delvaux - KU Leuven and Shanghai Jiao Tong U.
Dawu Gu - Shanghai Jiao Tong U.
Ingrid Verbauwhede – KU Leuven
- *A New Event-driven Dynamic Vision Sensor based Physical Unclonable Function for Camera Authentication in Reactive Monitoring System*
Yue Zheng, Yuan Cao and Chip Hong Chang - Nanyang Technological U.

- *Enhancing Noise Sensitivity of Embedded SRAMs for Robust True Random Number Generation in SoCs*
Md Tauhidur Rahman, Domenic Forte, and Mark Tehranipoor – U. of Florida
Xiaoxiao Wang – Beihang U.
- *RPUF: Physical Unclonable Function with Randomized Challenge to Resist Modeling Attack*
Jing Ye, Yu Hu and Xiaowei Li - Chinese Academy of Sciences
- *An Ultra-low Overhead LUT-based PUF for FPGA*
Jiadong Wang, Aijiao Cui, Mengyang Li - Harbin Institute of Technology Shenzhen Graduate School
Gang Qu – U. Maryland
Huawei Li – Chinese Academy of Sciences

12:00 – 1:20PM LUNCH

12:00 – 5:00PM POSTER SESSION (Note: in parallel with technical sessions)

12:30 – 12:50PM Lunch Talk

Speaker: Jason Sanabia, Raith America

Title: *Perfecting Large Area, High Resolution SEM Imaging with 3D-Stitching for Integrated Circuit Reverse Engineering*

1:20 – 1:50PM SESSION 3: INVITED TALK

Session Chair: Tsung-Yi Ho, National Tsing Hua University

Speaker: Masanori Hashimoto, Osaka University

Title: *Oscillator-based True Random Number Generator Robust to Process and Environmental Variation*

1:50 – 3:30PM SESSION 4: EMERGING HARDWARE SECURITY TOPICS

Session Chair: Shu-Min Li, National Sun Yat-sen University

- *Echeloned IJTAG Data Protection*
Senwen Kan – AMD
Jennifer Dworak and James George Dunham - Southern Methodist U.
- *Sneak Path Enabled Authentication for Memristive Crossbar Memories*
Md Badruddoja Majumder, Mesbah Uddin, and Garrett Rose – U. of Tennessee
Jeyavijayan Rajendran – U. of Texas at Dallas
- *Transistor-Level Camouflaged Logic Locking Method for Monolithic 3D IC Security*
Jaya Dofe and Qiaoyan Yu – U. of New Hampshire
Chen Yan, Scott Kontak, Emre Salman - Stony Brook U.
- *How Secure is Split Manufacturing in Preventing Hardware Trojan?*
Zhang Chen, Pingqiang Zhou - ShanghaiTech U.
Tsung-Yi Ho - National Tsing Hua U.

Yier Jin – U. of Central Florida

- *Using Image Sensor PUF as Root of Trust for Birthmarking of Perceptual Image Hash*
Yuan Cao – Hohai U.
Le Zhang and **Chip Hong Chang** - Nanyang Technological U.

3:30 – 3:50PM BREAK

3:50 – 5:30PM SESSION 5: HARDWARE PLATFORM ATTACK AND DEFENSE

Session Chair: Chip Hong Chang, Nanyang Technological University

- *Aging Attacks for Key Extraction on Permutation-Based Obfuscation*
Zimu Guo, Mark Tehranipoor and **Domenic Forte** – U. of Florida
- *Defeating Drone Jamming With Hardware Sandboxing*
Joshua Mead, Christophe Bobda and **Taylor Whitaker** – U. of Arkansas
- *A New Approach for Root-Causing Attacks on Digital Microfluidic Devices*
Pushpita Roy and **Ansuman Banerjee** - Indian Statistical Institute
- *Inner Collisions in ECC: Vulnerabilities of Complete Addition Formulas for NIST Curves*
Poulami Das, Debapriya Basu Roy, Harishma Boyapally and **Debdeep Mukhopadhyay** - IIT Kharagpur, India
- *Error Detection Reliable Architectures of Camellia Block Cipher Applicable to Different Variants of its Substitution Boxes*
Mehran Mozaffari Kermani - Rochester Institute of Technology
Reza Azarderakhsh - Florida Atlantic U.
Jiafeng Xie - Wright State U.

6:30 – 8:30PM DINNER (Evergreen Resort Hotel)

Tuesday, December 20, 2016

7:30 – 8:30AM Registration

SESSION 6: PLENARY SESSION

Moderator: Yier Jin, University of Central Florida

8:30 – 9:15AM KEYNOTE II

Speaker: Mark Tehranipoor, University of Florida

Title: *Security Rule Check: A New Automated Test for Security*

9:15 – 9:50AM INVITED TALK

Speaker: Shih-Lien Lu, TSMC

Title: *Hardware Security: A Foundry Perspective*

9:50 – 10:20AM BREAK

10:20AM – 12:00PM SESSION 7: SIDE-CHANNEL ATTACK AND COUNTERMEASURE

Session Chair: Pingqiang Zhou, ShanghaiTech University

- *Laser irradiation on EEPROM sense amplifiers enhances side-channel leakage of the bits being read*
Junichi Sakamoto, Daisuke Fujimoto and Tsutomu Matsumoto - Yokohama National U.
- *Key Extraction from the Primary Side of a Switched-Mode Power Supply*
Sami Saab, Andy Leiserson and Michael Tunstall - Rambus Cryptography Research
- *On-Chip Substrate-Bounce Monitoring for Laser-Fault Countermeasure*
Kohei Matsuda, Noriyuki Miura, Makoto Nagata - Kobe U.
Yu-Ichi Hayashi - Tohoku-Gakuin U.
Tatsuya Fujii and Kazuo Sakiyama – U. of Electro-Communications
- *Comparing Sboxes of Ciphers from the Perspective of Side-Channel Attacks*
Liran Lerman, Olivier Markowitch and Nikita Veshchikov - Université Libre de Bruxelles
- *Chosen Ciphertext Simple Power Analysis on Software 8-bit Implementation of Ring-LWE Encryption*
Aesun Park and Dong-Guk Han - Kookmin U.

12:00 – 1:00PM Lunch

1:00 – 1:30PM SESSION 8: INVITED TALK

Session Chair: Domenic Forte, University of Florida

Speaker: Yousef Iskander, CISCO

Title: *Ensuring System Integrity and Trust at Cisco*

1:30 – 2:50PM SESSION 9: HARDWARE TROJAN AND DETECTION

Session Chair: Kazuo Sakiyama, University of Electro-Communications

- *An Enhanced Classification-based Golden Chips-Free Hardware Trojan Detection Technique*
Mingfu Xue, Jian Wang - Nanjing U. of Aeronautics and Astronautics
Aiqun Hu - Southeast U.
- *Test Generation for Combinational Hardware Trojans*
Sying-Jyan Wang, Jhih-Yu Wei, Shih-Heng Huang - National Chung-Hsing U.
Katherine Shu-Min Li – National Sun Yat-sen U.

- *RECORD: Temporarily Randomized Encoding of Combinational Logic for Resistance to Data Leakage from Hardware Trojan*
Travis Schulze - Missouri U. of Science and Technology
Kevin Kwiat, Charles Kamhoua - Air Force Research Laboratory
Shih-Chieh Chang – National Tsing Hua U.
Yiyu Shi – U. of Notre Dame
- *Translating Circuit Behavior Manifestations of Hardware Trojans using Model Checkers into Run-time Trojan Detection Monitors*
Syed Rafay Hasan - Tennessee Tech U.
Charles Kamhoua, Kevin Kwiat and Laurent Njilla – Air Force Research Laboratory

2:50 – 3:50PM SESSION 9: INDUSTRIAL PANEL

Topic: *Hardware Security in Semiconductor Industry*

Panel Moderator: Gang Qu, University of Maryland

Panelists:

Ingrid Verbauwhede, KU Leuven

Jason Sanabia, Raith America

Shih-Lien Lu, TSMC

Yousef Iskander, CISCO

Garrett Rose, Univ. of Tennessee

Michael Mehlberg, Rambus

3:50 – 4:00M Closing Remarks

Sponsors:





HUAWEI

科技部

Ministry of Science and Technology