

AsianHOST 2019 Technical Program

AsianHOST 2019 Program Highlights

- 4 Featured Invited Speakers showcasing some of the world's leading innovative thinkers in hardware security! It includes 2 Keynote Talks and 2 Visionary Talks.
- 22 Technical Papers (16 Oral Presentations and 6 Poster Paper Presentations)
- Invited speakers:
 - Massimo Alioto – National University of Singapore, Singapore
 - Bernhard Lippmann - Infineon Technologies AG, Germany
 - Zhongyao Wen – Synopsys, USA
 - Yu Yao – Northeastern University, China
- A Student Poster Session (10 Student Posters)
- A Panel on Counterfeit Chip Detection

Sunday, December 15, 2019

5:30 PM - 7:30 PM **Welcome Reception @ 5th Floor Conference Room**

Monday, December 16, 2019

8:00 AM - 9:00 AM **Registration**

9:00 AM - 9:15 AM **Opening Remarks: AsianHOST 2019 General and Program Chairs**

9:15 AM - 10:00 AM **KEYNOTE 1**

Session Chair: Chip Hong Chang, Nanyang Technological University, Singapore

Speaker: Massimo Alioto, National University of Singapore

Title: *Ubiquitous Always-On Hardware Security: Trends, Perspectives and Directions*

10:00 AM - 10:30 AM **COFFEE BREAK**

10:30 AM - 11:50 AM **PAPER SESSION 1: HARDWARE ROOT OF TRUST**

Session Chair: Sheng Wei, Rutgers University, USA

- *VoltJockey: Breaking SGX by Software-Controlled Voltage-Induced Hardware Faults**
Pengfei Qiu, Dongsheng Wang, Yongqiang Lyu – Tsinghua Univ., China
Gang Qu – Univ. of Maryland, USA
- *Locking Secret Data in the Vault Leveraging Fuzzy PUFs**
Paul Shin, Yuan Cao – Hohai Univ., China
Xiaojin Zhao – Shenzhen Univ., China
Leilei Zhang – Fiberhome Telecommunication Technologies Co. Ltd, China
Fan Zhang – Zhejiang Univ., China

- *Identification of State Registers of FSM Through Full Scan by Data Analytics**
Chengkang He, Aijiao Cui – Harbin Institute of Technology (Shenzhen), China
Chip-Hong Chang – Nanyang Technological Univ., Singapore
- *RERTL: Finite State Transducer Logic Recovery at Register Transfer Level*
Jason Portillo, Travis Meade, John Hacker, Shaojie Zhang – Univ. of Central Florida, USA
Yier Jin – Univ. of Florida, USA
*Best Paper Award Candidate

11:50 AM - 1:15 PM LUNCH

1:15 PM - 1:45 PM VISIONARY TALK 1

Session Chair: Wei Hu, Northwestern Polytechnical University, China

Speaker: Zhongyao Wen, Synopsys, USA

Title: Security in Standard Interface Protocols

1:45 PM - 3:15 PM POSTER SESSION

Session Chair: Jiliang Zhang, Hunan University, China

SHORT PAPER POSTERS

- *Density-based Clustering Method for Hardware Trojan Detection Based on Gate-level Structural Features*
Pengyong Zhao and Qiang Liu – Tianjin Univ., China
- *Leveraging Unspecified Functionality in Obfuscated Hardware for Trojan and Fault Attacks*
Wei Hu, Yixin Ma, Xinmu Wang and Xingxin Wang – Northwestern Polytechnical Univ., China
- *An Orthogonal Algorithm for Key Management in Hardware Obfuscation*
Wang Jiawei, Zhang Yuejun – Ningbo Univ., China
Wang Pengjun – Wenzhou Univ., China
Luan Zhicun – Ningbo Univ., China
Xue Xiaoyong, Zeng Xiaoyang – Fudan Univ., China
Yu Qiaoyan – Univ. of New Hampshire, USA
- *Attack on a Microcomputer-Based Random Number Generator Using Auto-synchronization*
Salih Ergun – TÜBİTAK-Informatics and Information Security Research Center, Turkey
- *Low-Latency Pairing Processor Architecture Using Fully-Unrolled Quotient Pipelining Montgomery Multiplier*
Junichi Sakamoto, Yusuke Nagahama, Daisuke Fujimoto, Yota Okuaki and Tsutomu Matsumoto – Yokohama National Univ., Japan
- *Sweep to the Secret: A Constant Propagation Attack on Logic Locking*
Abdulrahman Alaql, Domenic Forte and Swarup Bhunia – Univ. of Florida, USA

STUDENT POSTERS

- *A Novel PUF Circuit Design Based on Slice for Autonomous Vehicles ECUs Authentication*
- *True Random Number Generator in 65nm CMOS Based on Chaotic System*
- *Portable Power Tracer for USIM*
- *RRAM based Flip-Flop Design for Secure Crypto Hardware*
- *Set-based Obfuscation for Strong PUFs against Machine Learning Attacks*
- *Design and Implementation of Leakage-Based PUF with High Reliability and Low-Cost*
- *Scan Chain based Aging Sensor for Detection of Recycled ICs*
- *A secure external IC metering scheme with low overhead*
- *Joint Gain Complement and Clustering-based Double-threshold Quantization for Physical Layer Key Generation*
- *A New Design of FSM State Register to Resist Fault Injection Attack*

3:15 PM - 3:45 PM COFFEE BREAK

3:45 PM - 4:15 PM VISIONARY TALK 2

Session Chair: Yuan Cao, Hohai University

Speaker: Yu Yao, Northeastern University, China

Title: *"Ditecting" Cyberspace Situation in Industrial Control Networks*

4:15 PM - 5:35 PM PAPER SESSION 2: SIDE CHANNEL AND PROBING ATTACKS

Session Chair: Fan (Terry) Zhang, Zhejiang University, China

- *Side-Channel-Attack Resistant Dual-Rail Asynchronous-Logic AES Accelerator Based on Standard Library Cells*
Kwen-Siong Chong, Aparna Shreedhar, Ne Kyaw Zwa Lwin, Nay Aung Kyaw, Weng-Geng Ho – Nanyang Technological Univ., Singapore
Chao Wang – Huazhong Univ. of Science and Technology, China
Jun Zhou – Univ. of Electronic Science and Technology of China
Bah-Hwee Gwee, Joseph Chang – Nanyang Technological Univ., Singapore
- *CAD4EM-P: Security-Driven Placement Tools for Electromagnetic Side Channel Protection*
Haocheng Ma – Tianjin Univ., China
Jiaji He – Tsinghua Univ., China
Yanjiang Liu, Yiqiang Zhao – Tianjin Univ., China
Yier Jin – Univ. of Florida, USA
- *Contact-to-Silicide Probing Attacks on Integrated Circuits and Countermeasures*
Qihang Shi, Haoting Shen and Domenic Forte – Univ. of Florida, USA
- *Fluctuating Power Logic: SCA Protection by VDD Randomization at the Cell-level*
Fan Zhang, Bolin Yang, Bojie Yang, Yiran Zhang – Zhejiang Univ., China
Shivam Bhasin – Nanyang Technological Univ., Singapore
Kui Ren – Zhejiang Univ., China

6:30 PM - 9:00 PM BANQUET AND AWARD CEREMONY

Tuesday, December 17, 2019

8:00 AM - 9:15 AM Registration

9:15 AM - 10:00 AM KEYNOTE 2

Session Chair: Yier Jin, University of Florida, USA

Speaker: Bernhard Lippmann, Infineon Technologies AG

Title: *Physical Verification of Advanced Semiconductor Products*

10:00 AM - 10:30 AM COFFEE BREAK

10:30 AM - 11:50 AM PAPER SESSION 3: DEEP LEARNING AND APPROXIMATE COMPUTING SECURITY

Session Chair: Qiang Liu, Tianjin University, China

- *Runtime Hardware Security Verification Using Approximate Computing: A Case Study on Video Motion Detection*
Mengmei Ye, Xianglong Feng and Sheng Wei – Rutgers Univ., USA
- *Vulnerability Analysis on Noise-Injection Based Hardware Attack on Deep Neural Networks*
Wenye Liu, Si Wang, and Chip-Hong Chang – Nanyang Technological Univ., Singapore
- *Detecting Adversarial Examples for Deep Neural Networks via Layer Directed Discriminative Noise Injection*
Si Wang, Wenye Liu, and Chip-Hong Chang – Nanyang Technological Univ., Singapore
- *Multi-label Deep Learning based Side Channel Attack*
Libang Zhang, Xinpeng Xing – Tsinghua Shenzhen International Graduate School, China
Junfeng Fan, Zongyue Wang, Suying Wang – Open Security Research, Inc., China

11:50 AM - 1:30 PM LUNCH

1:30 PM - 2:50 PM PAPER SESSION 4: PHYSICAL UNCLONABLE FUNCTION

Session Chair: Xiaolin Xu, University of Illinois at Chicago

- *A Modeling Attack Resistant Deception Technique for Securing PUF based Authentication*
Chongyan Gu – Queen Univ. Belfast, United Kingdom
Chip Hong Chang – Nanyang Technological Univ., Singapore
Weiqiang Liu – Nanjing Univ. Aeronautics and Astronautics, China
Shichao Yu – Queen Univ. Belfast, United Kingdom
Qingqing Ma – Nanjing Univ. Aeronautics and Astronautics, China
Maire O'Neill – Queen Univ. Belfast, United Kingdom

- *A Highly-Reliable and Energy-Efficient Physical Unclonable Function Based on 4T All-MOSFET Subthreshold Voltage Reference*
Peizhou Gan, Yiheng Wu – Shenzhen Univ., China
Yuan Cao – Hohai Univ., China
Xiaojin Zhao – Shenzhen Univ., China
- *Design of a Chaotic Oscillator based Model Building Attack Resistant Arbiter PUF*
Venkata Sreekanth Balijabudda, Dhruv Thapar, Pranesh Santikellur, Rajat Subhra Chakraborty and Indrajit Chakrabarti – India Institute of Technology Kharagpur, India
- *A Computationally Efficient Tensor Regression Network based Modeling Attack on XOR Arbiter PUF*
Pranesh Santikellur, Lakshya Lakshya, Shashi Ranjan Prakash and Rajat Subhra Chakraborty – India Institute of Technology Kharagpur, India

2:50 PM – 3:50 PM **PANEL**

Topic: *Hardware Anti-counterfeiting and Counterfeit Detection: State-of-the-art and Future Directions of Research*

Panel Moderator: Gang Qu - University of Maryland, USA
Panelists: Junfeng Fan - Open Security Research, China
 Yier Jin - University of Florida, USA
 Bernhard Lippmann - Infineon Technologies AG, Germany
 Zhongyao Wen - Synopsys, USA

3:50 PM - 4:00 PM **Closing Remarks**

Sponsors:



组 创 信 安