2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2021)

Shanghai, China
17 – 18 December 2021

IEEE

IEEE Catalog Number: CFP21F99-POD
ISBN: 978-1-6654-4186-5

IEEE Catalog Number:	CFP21F99-POD
ISBN (Print-On-Demand):	978-1-6654-4186-5
ISBN (Online):	978-1-6654-4185-8

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

AsianHOST 2021 Technical Program

AsianHOST 2021 Program Highlights

- 4 Featured Invited Speakers showcasing some of the world's leading innovative thinkers in hardware security!
- 20 Technical Papers (14 Oral Presentations and 6 Short Paper Presentations)
- Invited speakers:
  - Yongqiang Lyu, Tsinghua University, China
  - Maire O'Neill, Queen's University Belfast, United Kindom
  - Zhe Liu, Nanjing University of Aeronautics and Astronautics, China
  - Francois-Xavier Standaert, UC Louvain, Belgium
- A Student Poster Session (11 Student Posters)
- A Panel on Proliferating Hardware Security Ecosystem in Asia

---

December 17, 2021 (DAY 1)

9:00 AM - 9:15 AM Opening Remarks

9:15 AM - 9:50 AM Invited Talk 1
Session Chair: Xiaowei Li (Institute of Computing Technology, Chinese Academy of Sciences)/Pingqiang Zhou (ShanghaiTech University)

Speaker: Yongqiang Lyu, Tsinghua University, China
Title: *DVFS Transient Hardware Faults-Based Processor Security Threats*

9:50 AM - 10:05 AM BREAK

10:05 AM - 11:25 AM REGULAR PAPER SESSION 1: Advanced Hardware Attacks and Countermeasure
Session Chair: Fan Zhang (Zhejiang University)/Fu Song (ShanghaiTech University)

- *SSEL: An Extensible Specification Language for SoC Security.....1*
  Kshitij Raj, Arrush Hedge, Atul Prasad Deb Nath, Swarup Bhunia and Sandip Ray - University of Florida, USA

- *Ultra Freezing Attacks and Clock Glitching of Clock Oscillator Circuits.....7*
  Jonathon Durand, Anisul Abedin and Jakub Szefer - Yale University, USA

- *Revisiting UAV Authentication Schemes: Practical Attacks on Aviation Infrastructure.....13*
  Hirak Mondal and Urbi Chatterjee - Indian Institute of Technology, Kanpur, India

- *Detecting Adversarial Examples Utilizing Pixel Value Diversity.....19*
  Jinxin Dong and Pingqiang Zhou - ShanghaiTech University, China
  ** Best Paper Candidate*

LUNCH BREAK

1:15 PM - 2:15 PM REGULAR PAPER SESSION 2 - Side-Channel Attack and Countermeasure 1
Session Chair: Wei Hu (Northwestern Polytechnical University)/Jiliang Zhang (Hunan University)

- *Binary Classification-Based Side-Channel Analysis.....25*
  Chi Zhang, Xiangjun Lu and Dawu Gu - Shanghai Jiao Tong University, China

- *Deep Learning Side-Channel Attacks against Lightweight SCA Countermeasure RSM-AES.....31*
  Yuta Fukuda, Kota Yoshida, Hisashi Hashimoto and Takeshi Fujino - Ritsumeikan University, Japan

- *A Backpropagation Extreme Learning Machine Approach to Fast Training Neural Network-based Side-Channel Attack.....37*
  Xuyang Huang, Ming Ming Wong, Anh Tuan Do and Wang Ling Goh - Institute of Microelectronics (IME), A*STAR Singapore, Singapore

2:15 PM - 3:15 PM REGULAR PAPER SESSION 3 - Security Primitive Design
Session Chair: Weikang Qian (Shanghai Jiaotong University)/Xiaojin Zhao (Shenzhen University)

- *The Logic Obfuscation of LFSR with the Crosstalk based Polymorphic Gate.....43*
  Yuqian Sun, Xiaole Cui, Yongliang Chen and Xiaoxin Cui - Peking University Shenzhen Graduate School, China

- *An Ultra-low Power 3-T Chaotic Map based True Random Number Generator.....49*
  Lijuan Han, Yuan Cao, Lei Qian, Haodong Xie and Chip Hong Chang - Hohai University, China, Nanyang Technological University, Singapore
  ** Best Paper Award*

- *On Entropy and Bit Patterns of Ring Oscillator Jitter.....55*
  Markku-Juhani Saarinen – PQ Shield Ltd., UK

3:15 PM – 3:30 PM BREAK

3:30 PM - 4:05 PM Invited talk 2
Session Chair: Debdeep Mukhopadhyay (Indian Institute of Technology Kharagpur)/Weiqiang Liu (Nanjing University of Aeronautics and Astronautics)

Speaker: Maire O'Neill, Queen's University Belfast, United Kingdom
Title: *Physical Unclonable Functions - Challenge and Opportunities*

4:05 PM - 5:05 PM Panel
Topic: *Proliferating Hardware Security Ecosystem in Asia*
Panel Moderator: Chester Rebeiro (IIT Madras)

Panelists:

Junfeng Fan, Open Security Research, China
Debdeep Mukhopadhyay, IIT Kharagpur, India
Rajesh Pillai, SAG, DRDO, India
Ingrid Verbauwhede, KU Leuven, Belgium

December 18, 2021 (DAY 2)

9:00 AM - 9:35 AM Invited talk 3
Session Chair: Yuan Cao (Hohai University)/Pingqiang Zhou (ShanghaiTech University)

Speaker: Zhe Liu, Nanjing University of Aeronautics and Astronautics, China
Title: *Em-Curve25519: Faster and Smaller*

9:35 AM - 9:50 AM BREAK

9:50 AM - 10:50 AM PhD Forum
Session Chair: Weiqiang Liu (Nanjing University of Aeronautics and Astronautics)/Yingjie Lao (Clemson University)

- *Formal Analysis of Physically Unclonable Functions.....N/A*
  Durba Chatterjee, Debdeep Mukhopadhyay, Aritra Hazra - IIT Kharagpur, India

- *A Generic Dynamic Responding Mechanism and Secure Authentication Protocol for Strong PUFs.....N/A*
  Yale Wang, Chenghua Wang, Chongyan Gu, Yijun Cui, Maire O'Neill, Weiqiang Liu - Nanjing University of Aeronautics and Astronuatics, China, Queen's University Belfast, UK

- *True Random Number Generator with Conditional Perturbation using Stochastic Magnetic Tunnel Junction.....N/A*
  Jia-le Cui, Jun-tong Chen, Hao Cai - Southeast University, China

- *Hardware Acceleration for the Lattice-based Cryptography.....N/A*
  Weihang Tan - Clemson University, USA

- *Security Issues of Modern Image Processing Techniques in Lane Detection.....N/A*
  Shelaniece Clash - Morgan State University, USA

- *Fooling the Eyes of Autonomous Vehicles Using Physical Adversarial Examples.....N/A*
  Wei Jia, Haichun Zhang, Zhaojun Lu, Zhenglin Liu, Gang Qu - Huazhong University of Science and Technology, China, University of Maryland, USA

- *Metrics for Evaluating Fault Injection Attacks on Artificial Neural Networks.....N/A*
  Reetwik Das, Nikhilesh Singh, Chester Rebeiro - Indian Institute of Technology Madras, India

- *Memory Fault Detection For Deep Neural Networks.....N/A*
  Omid Aramoon - University of Maryland, USA

- *Deep Neural Network Training Data Protection against Model Inversion Attacks via Layer-Level Voltage Over-Scaling on Main Memory.....N/A*
  Qian Xu, Md Tanvir Arafin Gang Qu - University of Maryland College Park, Morgan State University, USA

- *A Platform for Structural Analysis of Logic Locking Using Machine Learning.....N/A*
  Prabuddha Chakraborty, Jonathan Cruz, Abdulrahman Alaql, and Swarup Bhunia - University of Florida, USA, King Abdulaziz City for Science and Technology, Saudi Arabia

- *Privacy Preserving Information Flow in Smart Grids.....N/A*
  Soumyadyuti Ghosh, Debdeep Mukhopadhyay, Soumyajit Dey - IIT Kharagpur, India

10:50 AM - 11:50 AM SHORT PAPER SESSION
Session Chair: Xin Lou (ShanghaiTech University)/Mingfu Xue (Nanjing University of Aeronautics and Astronautics)

- *Pipelined High-throughput NTT Architecture for Lattice-based Cryptography.....61*
  Weihang Tan, Antian Wang, Yingjie Lao, Xinmiao Zhang and Keshab Parhi - Clemson University, The Ohio State University, University of Minnesota, USA

- *A Novel Circuit Authentication Scheme based on Partial Polymorphic Gates.....65*
  Timothy Dunlap, Omid Aramoon, Gang Qu, Tian Wang, Xiaoxin Cui and Dunshan Yu - University of Maryland, USA, Peking University, China

- *Security Risk Assessment of Server Hardware Architectures using Graph Analysis.....69*
  Sandhya Koteshwara - IBM T.J. Watson Research Center, USA

- *Auto-PUFChain: An Automated Interaction Tool for PUFs and Blockchain in Electronic Supply.....73 Chain*
  Chandan Chaudhary, Urbi Chatterjee and Debdeep Mukhopadhyay - IIT, Kharagpur, IIT, Kanpur, India

- *Hardware Trojans Detection through RTL Features Extraction and Machine Learning.....77*
  Jizhong Yang, Ying Zhang, Yifeng Hua, Jiaqi Yao, Zhiming Mao and Xin Chen - Nanjing University Of Aeronautics And Astronautics, China

- *From FPGAs to Obfuscated eASICs: Design and Security Trade-offs.....81*
  Zain Ul Abideen, Tiago Diadami Perez and Samuel Pagliarini - Tallinn University of Technology, Estonia

LUNCH BREAK

1:15 PM - 2:35 PM REGULAR PAPER SESSION 4 - Side-Channel Attack and Countermeasure 2
Session Chair: Lingjuan Wu (Huazhong Agriculture University)/Jiaji He (Tianjin University)

- *Last-round and Joint First/Last-Round Power Analysis Attacks on PRESENT.....85*
  Qiang Fang and Massimo Alioto - National University of Singapore, Singapore

- *Attention-Based Non-Profiled Side-Channel Attack.....91*
  Xiangjun Lu, Chi Zhang and Dawu Gu - Shanghai Jiao Tong University, China

- *Revisiting System Noise in Side-Channel Attacks: Mutual Assistant SCA vs. Genetic Algorithm.....97*
  Rei Kudo, Takeshi Sugawara, Kazuo Sakiyama, Yuko Hara-Azumi and Yang Li - The University of Electro-Communications, Tokyo institute of Technology, Japan
  ** Best Paper Award*

- ***A Correlation Fault Attack on Rotating S-Box Masking AES.....103***
  Xingxin Wang, Jian Zheng, Lingjuan Wu, Jiacheng Zhu and Wei Hu - Northwestern Polytechnical University, Huazhong Agricultural University, China

2:35 PM – 2:50 PM BREAK

2:50 PM - 3:25 PM Invited talk 4
Session Chair: Debdeep Mukhopadhyay (Indian Institute of Technology Kharagpur)/Pingqiang Zhou (ShanghaiTech University)

Speaker: Francois-Xavier Standaert, UCLouvain, Belgium
Title: *Lessons From the Past, Challenges for the Future -- The Eurocrypt 2009 Evaluation Framework in the Deep Learning Era*

3:25 PM - 3:35 PM Closing Remarks and Awards Announcement

** All times are given in Beijing time*

Technical Sponsors

IEEE

HSTTC
IEEE Hardware Security & Trust Technical Committee

CEDA®
IEEE Council on Electronic Design Automation

上海科技大学
ShanghaiTech University

中国计算机学会 CCF

Platinum Sponsors

ICT 中国科学院计算技术研究所
INSTITUTE OF COMPUTING TECHNOLOGY, CHINESE ACADEMY OF SCIENCES