

2020 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2020)

**Kolkata, India
15 – 17 December 2020**



**IEEE Catalog Number: CFP20F99-POD
ISBN: 978-1-7281-8953-6**

**Copyright © 2020 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP20F99-POD
ISBN (Print-On-Demand):	978-1-7281-8953-6
ISBN (Online):	978-1-7281-8952-9

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

CURRAN ASSOCIATES INC.
proceedings
.com

AsianHOST 2018 Technical Program

Featured Speakers / Panelists



INVITED SPEAKER

Sharad Malik

Princeton University



INVITED SPEAKER

V. Kamakoti

Indian Institute of
Technology Madras



INVITED SPEAKER

Ingrid Verbauwhede

Research group COSIC,
KU Leuven



INVITED SPEAKER

Jason Fung

Intel Corporation

December 16, 2020 (DAY 1)

6:15 PM - 6:30 PM India Time (8:00AM - 8:15 EST) (9:00PM - 9:15PM Beijing Time) Opening Remarks from AsianHOST2020 General Chairs & PC Chairs

6:30 PM - 6:45 PM India Time (8:00AM - 8:15 EST) (9:00PM - 9:15PM Beijing Time) Introduction of the Hardware Security and Trust Technical Committee

Yao-Wen Chang, IEEE CEDA President

Gang Qu, IEEE HSTTC Co-Chair

Yier Jin, IEEE HSTTC Co-Chair

6:45 PM - 7:15 PM India Time (8:15AM - 8:45AM EST) (9:15PM - 9:45PM Beijing Time)

Pramod Subramanyan Memorial Lecture

Session Chair: Rajat Subhra Chakraborty, IITKGP

Speaker: Prof. Sharad Malik, Princeton University, USA

This lecture is dedicated to the memory and legacy of Pramad Subramanyan, who in a short span of a few years has left an indelible mark on the field of Hardware Security.

7:15PM - 8:00PM India Time (8:45AM - 9:30AM EST) (9:45PM - 10:30PM Beijing Time)

PAPER SESSION 1: HARDWARE ROOT OF TRUST

Session Chair: Ulrich Ruhmair, Ruhr University Bochum

HybridTEE: Secure Mobile DNN Execution Using Hybrid Trusted Execution Environment.....1

Akshay Gangal, Mengmei Ye and Sheng Wei - Rutgers, The State University of New Jersey, USA

Feedback-based Channel Gain Complement and Cluster-based Double-threshold Quantization for Physical Layer Key Generation.....7

Hang Liu, Chaofan Zhang, Hongming Fei, Wei Hu and Dawei Guo - Northwestern Polytechnique, Tshingua Univ, China

FPGA Accelerated Embedded System Security Through Hardware Isolation.....13

Sujan Kumar Saha and Christophe Bobda - Univ of Florida, USA

8:00PM - 8:15PM India Time (9:30AM - 9:45AM EST) (10:30PM - 10:45PM Beijing Time)
BREAK

8:15PM - 9:15PM India Time (9:45AM - 10:45AM EST) (10:45PM - 11:45PM Beijing Time)
PAPER SESSION 2: SIDE CHANNEL AND FAULT ATTACKS
Session Chair: Chester Rebeiro, IIT Madras

On The Deployment of Tweak-in-Plaintext Protection Against Differential Fault Analysis.....19
Jeroen Delvaux - Open Security Research, China

Revisiting the security of static masking and compaction: Discovering new vulnerability and Improved Scan Attack on AES.....25

Yogendra Sao, Dr. K.K.Soundra Pandian and Dr. Sk Subidh Ali - IIT Bhilai, India

PowerScout: A Security-Oriented Power Delivery Network Modeling Framework for Cross-Domain Side-Channel Analysis.....31

Huifeng Zhu, Xiaolong Guo, Yier Jin and Xuan Zhang - Washington University in St.Louis, Kansas State University USA, University of Florida USA

Revisiting Persistent Fault Analysis: Assessing Weak Keys and Strong Keys in Gift-64 Lightweight Cipher.....37

Arjit Arora, Kalpit Kothari, Priyanka Joshi and Bodhisatwa Mazumdar - IIT Indore, India

9:15PM - 9:30PM India Time (10:45AM - 11:00AM EST) (11:45PM - 12:00AM Beijing Time)
BREAK

9:30 PM - 10:00 PM India Time (11:00AM - 11:30AM EST) (12:00AM - 12:30AM Beijing Time) Keynote talk 2

Session Chair: Yier Jin, Univ of Florida, USA

Speaker: Mr. Jason Fung, Intel Corporation

10:00PM - 11:00PM India Time (11:30AM - 12:30PM EST) (12:30AM - 01:30AM Beijing Time)
SHORT PAPER SESSION

Session Chair: Shivam Bhasin,NTU Singapore

P2SA: Protecting Platoons from Stealthy Jamming Attack.....43

Yaodan Hu, Haoqi Shan, Raj Gautam Dutta and Yier Jin - University of Florida, USA

Defending Against Adversarial Attacks in Deep Learning with Robust Auxiliary Classifiers Utilizing Bit Plane Slicing.....49

Yuan Liu and Pingqiang Zhou - ShanghaiTech University, China

Malware Classification Through Attention Residual Network based Visualization.....53

Diangarti Bhalang Tariang, Sri Charan Birudaraju, Ruchira Naskar, Vijeta Khare and Rajat Subhra Chakraborty - IIT Kharagpur, IEST Shibpur, Adani Institute of Infrastructure Engineering, India

Danger Characterization of Electromagnetic Fault Injection on 32-bit Microcontroller Instruction Buffer.....59

Oualid Trabelsi, Laurent Sauvage and Jean-Luc - Télécom Paris, Institut Polytechnique de Paris, France

PUF Based Secure Framework for Hardware and Software Security of Drones.....65
Vishal Pal, Bharadwaj Amrutur, Ashish Joglekar, Srikrishna Acharya, Somesh Shrivastav and Sourav Saha - Indian Institute of Science, India

Model Inversion Defenses Using an Approximate Memory System.....71
Qian Xu, Md Tanvir Arafin and Gang Qu MIDAS - University of Maryland, College Park, Morgan State University USA

Defense against On-Chip Trojans Enabling Traffic Analysis Attacks.....75
M Meraj Ahmed, Abhijit Dhavle, Naseef Mansoor, Purab Sutradhar, Sai Manoj Pudukotai Dinakarrao, Kanad Basu and Amlan Ganguly - Rochester Institute of Technology, George Mason University, Minnesota State University, The University of Texas at Dallas, USA

Compact and Secure Generic Discrete Gaussian Sampler based on HW/SW Co-design.....81
Sudarshan Sharma, Arnab Bag and Debdeep Mukhopadhyay - IIT Kharagpur, India

December 17, 2020 (DAY 2)

6:30PM - 7:30 PM India Time (8:00AM - 9:00AM EST) (9:00PM - 10:00PM Beijing Time) PhD Forum

7:30 PM - 8:00 PM India Time (9:00AM - 9:30AM EST) (10:00PM - 10:30PM Beijing Time)

Keynote talk 3

Session Chair: Debdeep Mukhopadhyay, IIT Kharagpur, India

Speaker: Prof. Ingrid Verbauwhede, K. U. Leuven, Belgium

8:00PM - 8:45PM India Time (9:30AM - 10:15AM EST) (10:30PM - 11:15PM Beijing Time)

PAPER SESSION 3: LEAKAGE ANALYSIS USING FORMAL TOOLS & ML FOR SECURITY

Session Chair: Anupam Chattopadhyay, NTU Singapore

A Formal Framework for Gate-Level Information Leakage Using Z3.....87

Qizhi Zhang, Jiaji He, Yiqiang Zhao and Xiaolong Guo - Tianjin University, Tsinghua University, Kansas State University, USA

Hardware-Based Detection of Spectre Attacks: A Machine Learning Approach.....93

Yunjie Zhang and Yiorgos Makris - The University of Texas at Dallas, USA

Architecting a Secure Wireless Interconnect for Multichip Communication: An ML Approach...99

M Meraj Ahmed, Abhishek Vashist, Sai Manoj Pudukotai Dinakarrao and Amlan Ganguly - Rochester, GMU, USA

8:45PM - 9:00PM India Time (10:15AM - 10:30AM EST) (11:15PM - 11:30PM Beijing Time) BREAK

9:00PM - 9:45PM India Time (10:30AM - 11:15AM EST) (11:30PM - 12:15AM Beijing Time)

PAPER SESSION 4: LOGIC LOCKING AND PUFs

Session Chair: Subidh Ali, IIT Bhilai

SAT Based Partial Attack on Compound Logic Locking.....105

Melbin John, Aadil Hoda, Ramanuj Chouksey and Chandan Karfa - IIT Guwahati, India

Security Primitive Generator for RT-Level Logic Locking and Watermarking.....111

Jun Kuai, Jiayi He, Haocheng Ma, Yiqiang Zhao, Yumin Hou and Yier Jin - Tianjin University, China, Tsinghua University, China, University of Florida, USA

Boosting Entropy and Enhancing Reliability for Physically Unclonable Functions.....117

Ricardo Valles-Novo, Andres Martinez-Sanchez and Wenjie Che - New Mexico State Univ, USA

9:45PM - 10:00PM India Time (11:15AM - 11:30AM EST) (12:15AM - 12:30AM Beijing Time)
BREAK

10:00 PM - 10:30 PM India Time (11:30AM - 12:00PM EST) (12:30AM - 01:00AM Beijing Time) Keynote talk 4

Session Chair: Pingqiang Zhou, Shanghai-Tech

Speaker: Prof. V Kamakoti, IIT Madras

10:30PM - 11:30PM India Time (12:00PM - 1:00PM EST) (1:00AM - 2:00AM Beijing Time)

PANEL DISCUSSION

Topic: *AI for Hardware Security: Boon or Bane*

Panel Moderator: Chester Rebeiro, Indian Institute of Technology Madras, India

Panelists:

Avi Mendelson, Technion, Israel

Stjepan Picek, Delft University of Technology, Netherlands

Domenic Forte, University of Florida, USA

Rosario Cammarota, Intel Corporation

Lejla Batina, Radboud University, Netherlands

11:30PM - 11:40PM India Time (1:00PM - 1:10PM EST) (02:00AM - 02:10AM Beijing Time)
CONCLUDING REMARKS