2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2018)

Hong Kong
17 – 18 December 2018

IEEE Catalog Number: CFP18F99-POD
ISBN: 978-1-5386-7472-7

****** 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:	CFP18F99-POD
ISBN (Print-On-Demand):	978-1-5386-7472-7
ISBN (Online):	978-1-5386-7471-0

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

AsianHOST 2018 Program Highlights

- 5 Featured Invited Speakers showcasing some of the world's leading innovative thinkers in hardware security! It includes 2 Keynote Talks and 3 Visionary Talks.
- 19 Technical Papers
- Invited speakers:
  - Makoto Ikeda - University of Tokyo
  - Ahmad-Reza Sadeghi - Technische Universität Darmstadt
  - Marilyn Wolf - Georgia Tech
  - Naehyuck Chang - Korea Advanced Institute of Science and Technology (KAIST)
  - Sandip Kundu – National Science Foundation and University of Massachusetts, Amherst
- A Panel on Hardware Supply Chain Security

Sunday, December 16, 2018

5:00 - 7:00PM Conference Reception @ Conference Lodge

Monday, December 17, 2018

8:00 - 9:00AM Registration @ Institute for Advanced Study (IAS)

SESSION 1: PLENARY SESSION
Moderator: Tim Cheng, Dean of Engineering, Hong Kong University of Science and Technology

9:00 - 9:15AM Opening Remarks: AsianHOST 2018 General and Program Chairs

9:15 - 10:00AM KEYNOTE 1
Speaker: Makoto Ikeda, University of Tokyo
Title: *Exploring Elliptic Curve based cryptography hardware design .....N/A*

10:00 - 10:30AM COFFEE BREAK

10:30 - 11:50AM SESSION 2: HARDWARE-ORIENTED ATTACKS
Session Chair: Wei Hu, Northwestern Polytechnical University

- *An Efficient Hardware-Oriented Runtime Approach for Stack-based Software Buffer Overflow Attacks**.....1
  Love Sah, Sheikh Ariful Islam and Srinivas Katkoori – Univ. of South Florida

- *Probing Attacks on Key Agreement for Automotive Controller Area Networks** **.....7**
  Shalabh Jain – Bosch Research and Technology Center
  Qian Wang, and Md Tanvir Arafin – Univ. of Maryland
  Jorge Guajardo Merchan – Robert Bosch LLC, RTC, USA

- *Modeling and Efficiency Analysis of Clock Glitch Fault Injection Attack* **.....13**
  Bo Ning and Qiang Liu – Tianjin Univ.

- *A Wavelet-based Power Analysis Attack against Random Delay Countermeasure* **.....19**
  Xiaofei Dong, Fan Zhang, Samiya Queshi, Yiran Zhang, Ziyuan Liang and Feng Gao

  – Zhejiang Univ.

*** Best Paper Candidate**

11:50AM - 1:30PM LUNCH

1:30 – 2:00PM SESSION 3: VISIONARY TALK 1
Moderator: Yier Jin, University of Florida

Speaker: Sandip Kundu, NSF and University of Massachusetts, Amherst
Title: *Adversarial Attacks on Machine Learning Systems***.....N/A**

2:00 - 3:20 PM SESSION 4: PHYSICAL UNCLONABLE FUNCTION
Session Chair: Jia Di, University of Arkansas

- *Defeating Strong PUF Modeling Attack via Adverse Selection of Challenge-Response Pairs* 25*
  Horácio França – UFRJ
  Charles Prado – National Institute of Metrology, Quality and Technology
  Vinay Patil and Sandip Kundu – Univ. of Massachusetts Amherst

- *Bias PUF based Secure Scan Chain Design 31*
  Wenjie Li, Jing Ye, Xiaowei Li, Huawei Li and Yu Hu – Chinese Academy of Sciences

- *The Cell Dependency Analysis on Learning SRAM Power-Up States 37*
  Zhonghao Liao and Yong Guan – Lowa State Univ.

- *Generation of PUF-keys on FPGAs by K-means Frequency Clustering 44*
  Asha K A, Abhishek Patyal and Hung-Ming Chen – National Chiao Tung Univ.

3:20 - 3:50PM COFFEE BREAK

3:50 - 4:20PM SESSION 5: VISIONARY TALK 2
Moderator: Gang Qu, University of Maryland

Speaker: Naehyuck Chang, KAIST
Title: *Design Automation of Low-Power Cyber-Physical Systems .....N/A*

4:20 - 5:40PM SESSION 6: MACHINE LEARNING ON HARDWARE SECURITY
Session Chair: Haihua Shen, University of Chinese Academy of Sciences

- *Machine Learning Attacks on VOS-based Lightweight Authentication 50*
- **Jiliang Zhang – Hunan Univ.**

- *SAIL: Machine Learning Guided Structural Analysis Attack on Hardware Obfuscation 56*
- **Prabuddha Chakraborty, Jonathan Cruz and Swarup Bhunia – Univ. of Florida**

- *Preventing Neural Network Model Exfiltration in Machine Learning Hardware Accelerators* **.....62**
  Mihailo Isakov, Lake Bu, Hai Cheng and Michel Kinsy - Boston Univ.

- *Detecting RTL Trojans using Artificial Immune Systems and High-Level Behavior Classification* **.....68**
  Farhath Zareen and Robert Karam – Univ. of South Florida

6:00 - 8:30PM BANQUET AND AWARD CEREMONY @ China Gardens
Ceremony Moderators:
Tim Cheng, Dean of Engineering, Hong Kong University of Science and Technology
Wei Zhang, Hong Kong University of Science and Technology
Gang Qu, Professor, University of Maryland
Best Paper Moderator:
Qiang (Johnny) Xu, The Chinese University of Hong Kong

Tuesday, December 18, 2018

8:30 - 9:00AM Registration

9:00 – 10:15AM SESSION 7: PLENARY SESSION
Moderator: Qiang (Johnny) Xu, The Chinese University of Hong Kong

9:00 - 9:45AM KEYNOTE 2
Speaker: Ahmad-Reza Sadeghi, TU Darmstadt
Title: *Mind the Gap: Promises, Pitfalls, and Opportunities of Hardware-Assisted Security .....N/A*

9:45 - 10:15AM VISIONARY TALK 3
Speaker: Marilyn C. Wolf, Georgia Tech
Title: *Design Processes for Security and Safety* .....N/A

10:15 - 10:40AM COFFEE BREAK

10:40AM - 12:00PM SESSION 8: PREVENTIVE COUNTERMEASURES
Session Chair: Yongqiang Lyu, Tsinghua University

- *Cost-efficient 3D Integration to Hinder Reverse Engineering During and After Manufacturing 74*
  Peng Gu, Dylan Stow, Prashansa Mukim, Shuangchen Li and Yuan Xie – UCSB

- *Secrecy Performance of Cognitive Radio Sensor Networks with an Energy-Harvesting based Eavesdropper and Imperfect CSI 80*
  Rongjun Tan, Yuan Gao, Haixia He and Yuan Cao – Hohai Univ.

- *A Delay based Plug-in-Monitor for Intrusion Detection in Controller Area Network 86*
  Qian Wang, Yiming Qian, Gang Qu and Yasser Shoukry – Univ. of Maryland
  Zhaojun Lu – Huazhong Univ. of Science and Technology

- *A Novel Lightweight Hardware-assisted Static Instrumentation Approach for ARM SoC Using Debug Components* **.....92**
  Muhammad Abdul Wahab, Mounir Nasr Allah, and Guillaume Hiet – CentraleSupélec
  Pascal Cotret – independent researcher
  Vianney Lapotre, Guy Gogniat – Université de Bretagne-Sud
  Arnab Kumar Biswas – UBS

12:00 - 1:30PM LUNCH

1:30 - 2:30PM SESSION 9: VULNERABILITY ANALYSIS
Session Chair: Sheng Wei, University of Rutgers

- *A Comprehensive Analysis on Vulnerability of Active Shields to Tilted Microprobing Attacks 98*
  Qihang Shi, Huanyu Wang, Navid Asadizanjani, Mark Tehranipoor and Domenic Forte – Univ. of Florida

- *Ring Oscillator Based Random Number Generator Using Wake-up and Shut-down Uncertainties* **.....104**
  Mehmet Alp Şarkışla – TUBITAK
  Salih Ergun – ERGTECH Research Center

- *Empirical Word-Level Analysis of Arithmetic Module Architectures for Hardware Trojan Susceptibility* **.....109**
  Sheikh Ariful Islam, Srinivas Katkoori and Love Kumar Sah – Univ. of South Florida

2:30 – 3:30PM SESSION 10: PANEL
Topic: *Hardware Supply Chain Security in Asia and Around the World .....N/A*
Panel Moderator: Gang Qu, University of Maryland
Panelists:
Tim Cheng - Hong Kong University of Science and Technology
Yousef Iskander - Cisco
Sandip Kundu - National Science Foundation and University of Massachusetts, Amherst
Haihua Shen - University of Chinese Academy of Sciences
Mark Tehranipoor - University of Florida
Marilyn Wolf - Georgia Tech

3:30 - 3:45PM Closing Remarks