2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2024)

Washington, DC, USA
6-9 May 2024

IEEE Catalog Number: CFP24HOA-POD
ISBN: 979-8-3503-7395-0

****** 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:	CFP24HOA-POD
ISBN (Print-On-Demand):	979-8-3503-7395-0
ISBN (Online):	979-8-3503-7394-3
ISSN:	2835-5709

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

Technical Program

Tutorials

Monday, 6th May 2024

09:30 – 12:00	**TUTORIALS 1 & 2** **Tutorial 1. Hardware Security and Trust Verification...N/A** **Prabhat Mishra** – University of Florida **Ankur Srivastava** – University of Maryland **Tutorial 2. Post-Quantum Cryptography: Implementation Attacks and Countermeasures...N/A** **Daniel Dinu** – Intel Corporation **Prasanna Ravi** – Nanyang Technological University, Singapore **Markku-Juhani Saarinen** – Tampere University, Finland
12:00 – 13:00	**Break & Lunch**
13:00 – 14:30	**TUTORIALS 3 & 4** **Tutorial 3. Explainable AI for Cybersecurity...N/A** **Zhixin Pan** – Florida State University **Prabhat Mishra** – University of Florida **Tutorial 4. Security of Quantum Computing Systems...N/A** **Jakub Szefer** – Yale University
14:30 – 15:00	**Break**
15:00 – 17:30	**TUTORIALS 5 & 6** **Tutorial 5. Heterogeneous Integration Security...N/A** **Farimah Farahmandi** – University of Florida **Mark Tehranipoor** – University of Florida **Tutorial 6. Tabletop exercise – Risks of a Trust-based Supply Chain...N/A** **Ahalya Sankararaman** – University of Waterloo **Sebastian Fischmeister** – University of Waterloo

Tuesday, 7th May 2024

07:00 – 08:10	**Breakfast**
07:30 – 17:30	**Registration**
08:30 – 18:00	**Exhibits Demo-Posters**
08:10 – 08:30	**Opening Remarks: HOST 2024 General and Program Chairs**
08:30 – 09:10	**Session 1: Keynote Address** **Session Chair:** Mark Tehranipoor (University of Florida) **Title**: The CHIPS R&D Program...N/A **By**: Greg Yeric (Director of Research, CHIPS NSTC program)
09:10 – 10:10	**Session 2: Side-channel Leakage with Machine Learning** **Session Chair:** Fareena Saqib (UNC Charlotte) ***2.1. NoiseHopper: Emission Hopping Air-Gap Covert Side Channel with Lower Probability of Detection...21** *Authors: Md Faizul Bari and Shreyas Sen* ***2.2. TinyPower: Side-Channel Attacks with Tiny Neural Networks...320** *Authors: Haipeng Li, Mabon Ninan, Boyang Wang and John Emmert* **2.3. SNOW-SCA: ML-assisted Side-Channel Attack on SNOW-V...139** *Authors: Harshit Saurabh, Anupam Golder, Samarth Shivakumar Titti, Suparna Kundu, Chaoyun Li, Angshuman Karmakar and Debayan Das* **HOST 2024 Best Paper Nominee*
10:10 – 10:30	**AM Break**
10:30 – 11:00	**Session 3: Visionary Talk 1** **Session Chair**: Kanad Basu (UT Dallas) **By** Ophir Gaathon (Co-founder and CEO, DUST Identity) **Title:** Building Trust in Complex Global Supply Chains...N/A
11:00 – 12:00	**Session 4: Pre-silicon Security Verification and Validation** **Session Chair:** Soheil Salehi (University of Arizona) **4.1. Prioritizing Information Flow Violations: Generation of Ranked Security Assertions for Hardware Designs...128** *Authors: Avinash Ayalasomayajula, Nusrat Farzana Dipu, Debjit Pal and Farimah Farahmandi* **4.2. Verifying Memory Confidentiality and Integrity of Intel TDX Trusted Execution Environments...44** *Authors: Hasini Dllanka, Debapriya Chatterjee and Prabhat Mishra* **4.3. RTL-Spec: RTL Spectrum Analysis for Security Bug Localization...171** *Authors: Samit Miftah, Shamik Kundu, Mordahi Austin, Shiyi Wei and Kanad Basu*

12:00 – 13:00	**Lunch Break**
13:00 – 13:40	**Session 5: Keynote Address** **Session Chair**: Ioannis Savidis (Drexel University) **By** George Orji (Deputy Director, NIST NAPMP) **Title:** CHIPS-NAPMP: Overview and Next Steps...N/A
13:40 – 15:00	**Session 6: Hide Behind Masks** **Session Chair:** Naghmeh Karimi (University of Maryland, Baltimore County) **6.1. Masked Memory Primitive for Key Insulated Schemes...293** *Authors: Zachary DiMeglio, Jenna Bustami, Deniz Gurevin, Chenglu Jin, Marten van Dijk and Omer Khan* ***6.2. DOMREP II...112** *Authors: Matthias Probst, Manuel Brosch, Michael Gruber and Georg Sigl* ***6.3. Security Aspects of Masking on FPGAs...199** *Authors: Barbara Gigerl, Kevin Pretterhofer and Stefan Mangard* **6.4. Randomization approaches for Secure SAR ADC design resilient against Power Side-Channel Attacks...282** *Authors: Sumanth N Karanth, Sirish Oruganti, Meizhi Wang and Jaydeep P Kulkarni* **HOST 2024 Best Paper Nominee*
15:00 – 16:30	**Session 7: PM Break + Hardware Demos Session 1 + Poster Presentations** Poster Titles: 1. Cache Wars: A Comparative Study of UMWAIT, UMONITOR, and Prime-Probe Attacks...86 2. Trained to Leak: Hiding Trojan Side-Channels in Neural Network Weights...122 3. Towards Practical Fabrication Stage Attacks Using Interrupt-Resilient Hardware Trojans...254 4. A Lightweight Non-Oscillatory Delay-Sensor for Remote Power Analysis...343 5. Too Hot to Handle: Novel Thermal Side-Channels in Power Attack protected Intel processors...378
16:30 – 17:10	**Session 8: Keynote Address** **Session Chair**: Ankur Srivastava (University of Maryland) **By** Dev Shanoy (OUSD R&E) **Title:**DoD's Microelectronics Hardware Security: Vision, Strategy, and Implementation...N/A
17:10 – 18:00	**Exhibitors Presentations + Poster Presentations**

17:15 – 17:25: JIACO
Title: Preserving Stored Data and Device Functionality After Decapsulation Using Atmospheric Microwave Induced Plasma...N/A
Presenter: Mark McKinnon (Sales Director, JIACO Instruments)

17:30 – 17:40: Riscure
Title: Post-Quantum Crypto on Embedded Devices...N/A
Presenter: Cameron Howell (Security Analyst)

IEEE International Symposium on Hardware Oriented Security and Trust (HOST)
Washington DC, USA
May 6-9, 2024
PROCEEDINGS

Wednesday, 8th May 2024

07:00 – 08:10	**Breakfast**
07:30 – 17:30	**Registration**
08:00 – 16:15	**Exhibits Demos**
08:30 – 11:00	**Ph.D. Dissertation challenge: Will be scheduled in parallel with the program in one of the meeting rooms**
08:10 – 08:20	**Plenary Session**
08:20 – 09:00	**Session 9: Keynote Address** **Session Chair**: Farimah Farahmandi (University of Florida) **By** Suzy Ramirez Greenberg (Vice President of Intel Product Assurance and Security and General Manager of Product Incident Response and Communications, Intel) **Title:** Security is a Mindset, Not Just A Feature...N/A
09:00 – 10:00	**Session 10: Neural Network Security** **Session Chair:** Sazadur Rahman (University of Central Florida) **10.1. QNAD: Quantum Noise Injection for Adversarial Defense in Deep Neural Networks...1** *Authors: Shamik Kundu, Navnil Choudhury, Sanjay Das, Arnab Raha and Kanad Basu* **10.2. One Flip Away from Chaos: Unraveling Single Points of Failure in Quantized DNNs...332** *Authors: Cheng Gonge and Yunsi Fei* **10.3. Explainability to the Rescue: A Pattern-Based Approach for Detecting Adversarial Attacks...160** *Authors: Sanjas Das, Shamik Kundu and Kanad Basu*
10:00 – 10:30	**AM Break**
10:30 – 11:50	**Session 11: SoCs that Don't SoC!!** **Session Chair:** Hadi Mardani Kamali (University of Central Florida) **11.1. Empowering Hardware Security with LLM: The Development of a Vulnerable Hardware Database...233** *Authors: Dipayan Saha, Katayoon Yahyaei, Sujan Kumar Saha, Mark Tehranipoor and Farimah Farahmandi* **11.2. LightEMU: Hardware Assisted Fuzzing of Trusted Applications...420** *Authors: Dean Sullivan, Haoqi Shan, Sravani Nissankararao, Shup Wang, Yier Jin, Moyao Huang and Yujaia Liu* **11.3. DiSPEL: A Framework for SoC Security Policy Synthesis and Distributed Enforcement...271** *Authors: Sudipta Paria, Aritra Dasgupta and Swarup Bhunia* **11.4. MaliGNNoma: GNN-Based Malicious Circuit Classifier for Secure**

	Cloud FPGAs...383 *Authors: Lilas Alrahis, Hassan Nassar, Jonas Krautter, Dennis Gnad, Lars Bauer, Jorg Henkel and Mehdi Tahoori*
11:50 – 13:00	**Lunch Break**
13:00 – 14:20	**Session 12: Post-Quantum Hardware Security** **Session Chair:** Reza Azarderakhsh (Florida Atlantic University) **12.1. A High Efficiency Hardware Design for the Post-Quantum KEM HQC...431** *Authors: Francesco Antognazza, Alessandro Barenghi, Gerardo Pelosi and Ruggero Susella* **12.2. A Thorough Study of State Leakage Mitigation in Quantum Computing with One-Time Pad...55** *Authors: Chuanqi Xu, Jamie Sikora and Jakub Szefer* **12.3. A Hardware-Software Co-Design for the Discrete Gaussian Sampling of FALCON Digital Signature...90** *Authors: Emre Karabulut and Aydin Aysu* **12.4. Sparse Polynomial Multiplication-based High-Performance Hardware Implementation for CRYSTALS-Dilithium...150** *Authors: Hang Zhao, Cankun Zhao, Wenping Zhu, Bohan Yang, Shaojun Wei and Leibo Liu*
14:20 – 15:50	**Session 13: Exhibits, Hardware Demo Session 2 + PM Break + Poster Presentations** Poster Titles: 1. FitBit: Ensuring Robust and Secure Execution through Runtime-generated Stressmarks...194 2. LightFAt: Mitigating Control-flow Explosion via Lightweight PMU-based Control-Flow Attestation...222 3. CTR+: A High-Performance Metadata Access Scheme for Secure Embedded Memory in Heterogeneous Computing Systems...304 4. Voltage Noise-Based Adversarial Attacks on Machine Learning Inference in Multi-Tenant FPGA Accelerators...80 5. Data-Oblivious ML Accelerators using Hardware Security Extensions...373 6. DOSCrack: Deobfuscation using Oracle-guided Symbolic execution and Clustering of binary security keys...227
15:50 – 16:30	**Session 14: Keynote Address** **Session Chair**: Aydin Aysu (NC State University) **By** Jayson Bethurem (VP, Marketing and Business Development, Flex Logix) **Title:**Enable Long-lasting SoC Security with Crypto Agility
16:30 – 17:45	**Session 15: Panel 1** **Title:** Riding the Wave: The Thin Line Between Fortifying AI Hardware and Unleashing Its Potential...N/A

	Panelists: **Eric Breckenfeld** (Nvidia) **Ioannis Savidis** (Drexel University) **Guerney Hunt** (IBM) **Matt Casto** (MMEC)
17:45 – 18:30	**Break + Demos + Poster Presentations**
18:30 – 20:30	**Session 16: Banquet and Award Ceremony**

Thursday, 9th May 2024

07:00 – 08:20	**Breakfast**
07:30 – 12:30	**Registration**
08:20 – 08:30	**Plenary Session**
08:30 – 09:00	**Session 17: Visionary Talk 2** **Session Chair**: Ioannis Savidis (Drexel University) **By** Vivek Menon (Mission Assurance Director, NRO) **Title:** R.I.P. Logic Locking! Re-examining Threat Vectors with CHIPS Act...N/A
09:00 – 10:20	**Session 18: System Security** **Session Chair:** Ujwall Guin (Auburn University) **18.1. RowHammer Cache: A Last-level Cache for Low-Overhead Row-Hammer Tracking...349** *Authors: Aman Singh and Biswabandan Panda* **18.2. TrustZoneTunnel: A Cross-world Pattern History Table-based Microarchitectural Side-channel Attack...260** *Authors: Tianhong Xu, Yunsi Fei and Aidong Adam Ding* **18.3. Resurrection Attack: Defeating Xilinx MPU's Memory Protection...394** *Authors: Bharadwaj Madabhushi, Chandra Sekhar Mummidi, Sandip Kundu and Daniel Holcomb* **18.4. A Security Assessment of Protected Execute-only Firmware in Microcontrollers through Selective Chemical Engraving...12** *Authors: Xiaomei Zeng, Qing Liu, Samuel Chef and Chee Lip Gan*
10:20 – 11:00	**Session 19: AM Break + Poster Presentations** Poster Titles: 1. A Pre-Silicon Physical Design Study Towards Mitigating EMSCA on Cryptographic ICs...66 2. Breaking SCA-Protected CRYSTALS-Kyber with a Single Trace...70 3. Time-Aware Re-Synthesis for Secure Quantum Systems...74 4. All Your Base Are Belong To Us: Stealing VRP Secrets from Quantum Circuit Structures...415 5. Photon Emission Modeling and Machine-Learning Assisted Pre-Silicon Optical Side-channel Simulation...107 6. Covert Communication Channels Based On Hardware Trojans: Open-Source Dataset and AI-based Detection...101
11:00 – 12:00	**Session 20: Quantum and Side-Channel** **Session Chair:** Jiafeng "Harvest" Xie (Villanova University) **20.1. Charlie, Charlie, Charlie on Industrial Control Systems: PLC Control Logic Attacks by Design, Not by Chance...182**

	Authors: Adeen Ayub, Wooyeon Jo and Irfan Ahmed **20.2. Calibratable Polymorphic Temperature Sensor for Detecting Side channel and Fault Injection Attacks...211** *Authors: Tasnuva Farheen, Sourav Roy, Jia Di, Shahin Tajik and Domenic Forte* **20.3. Dynamic Pulse Switching for Protection of Quantum Computation on Untrusted Clouds...404** *Authors: Theodoros Trochatos, Sanjay Deshpande, Chuanqi Xu, Yao Lu, Yongshan Ding and Jakub Szefer*
12:00 – 13:30	**Lunch Break** **Session 21: Panel 2: Guardians of the Chips: The Challenge in Closing the Workforce Gap** **Moderator: Mike Kines** (OSU) **Panelists:** **Antonio De La Serna** (Siemens) **Patty Schaefer** (BAH) **Jeyavijayan "JV" Rajendran** (Texas A&M U) **Adam Kimura** (Battelle) **Joe Sweeney** (Amazon)
13:30 – 14:50	**Session 22: Choose Your PUF Wisely!** **Session Chair:** Ryan Helinski (Sandia National Laboratories) **22.1. SpongePUF: A Modeling Attack Resilient Strong PUF with Scalable Challenge Response Pair...244** *Authors: Zhenzhe Chen, Takashi Sato and Hirofumi Shinohara* **22.2. PhenoAuth:A Novel PUF-Phenotype-based Authentication Protocol for IoT Devices...309** *Authors: Fei Hongming, Prosanta Gope, Owen Millwood, Jack Miskelly and Biplab Sikdar* **22.3. Machine Learning Attacks on Challenge-Response Obfuscations in Strong PUFs...361** *Authors: Neelofar Hassan and Urbi Chatterjee* **22.4. Non-Invasive Attack on Ring Oscillator-based PUFs through Localized X-Ray Irradiation...33** *Authors: Nasr-Eddine Ouldei Tebina, Aghiles Douadi, Luc Salvo, Vincent Beroulle, Nacer-Eddine Zergainoh, Guillaume Hubert, Ioana Vatajelu, Giorgio Di Natale and Paolo Maistri*
14:50 – 15:00	**Concluding Remarks** **Program and General Chairs 2024/2025**