

# **2024 International Symposium on Secure and Private Execution Environment Design (SEED 2024)**

**Orlando, Florida, USA  
16-17 May 2024**



**IEEE Catalog Number: CFP24Z58-POD  
ISBN: 979-8-3315-0566-0**

**Copyright © 2024 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:	CFP24Z58-POD
ISBN (Print-On-Demand):	979-8-3315-0566-0
ISBN (Online):	979-8-3315-0565-3

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2024 International Symposium on Secure and Private Execution Environment Design (SEED) **SEED 2024**

## Table of Contents

Message from the General Chairs .....	viii
Message from the Program Chairs .....	ix
Organizing Committee .....	x
Program Committee .....	xi
Steering Committee .....	xii

### Session 1: Side Channel Attacks

Extending FPGA Information Leaks with Trojan Phantom Circuits .....	1
<i>Anthony Etim (Yale University, USA), Shanquan Tian (Yale University, USA), and Jakub Szefer (Yale University, USA)</i>	
Tail Victims in Termination Timing Channel Defenses Beyond Cryptographic Kernels .....	11
<i>Shijia Wei (The University of Texas at Austin, United States), Austin Harris (The University of Texas at Austin, United States), Yongye Zhu (University of California, Berkeley, United States), Prakash Ramrakhyani (ARM, United States), Calvin Lin (The University of Texas at Austin, United States), and Mohit Tiwari (The University of Texas at Austin, United States)</i>	
Channelizer: Explainable ML Inference for Validating Side-Channel Resistant Systems .....	23
<i>Donayam Benti (University of Michigan, USA) and Todd Austin (University of Michigan, USA)</i>	
Beyond the Bridge: Contention-Based Covert and Side Channel Attacks on Multi-GPU Interconnect .....	35
<i>Yicheng Zhang (University of California, United States), Ravan Nazaraliyev (University of California, United States), Sankha Baran Dutta (Pacific Northwest National Laboratory, United States), Nael Abu-Ghazaleh (Pacific Northwest National Laboratory, United States), Andres Marquez (Pacific Northwest National Laboratory, United States), and Kevin Barker (Pacific Northwest National Laboratory, United States)</i>	

## Session 2: Hardware-Based Defenses

INTERFACE: An Indirect, Partitioned, Random, Fully-Associative Cache to Avoid Shared Last-Level Cache Attacks .....	37
<i>Yonas Kelemework (Intel Corporation, Canada) and Alaa R. Alameldeen (Simon Fraser University, Canada)</i>	
MAYA: Hardware Enhanced Customizable Defenses at the User-Kernel Interface .....	50
<i>Preet Derasari (George Washington University, USA) and Guru Venkataramani (George Washington University, USA)</i>	
A First Exploration of Fine-Grain Coherence for Integrity Metadata .....	62
<i>Per Ekemark (Uppsala University, Sweden), Alberto Ros (Universidad de Murcia, Spain), Konstantinos Sagonas (Uppsala University, Sweden; National Technical University of Athens, Greece), and Stefanos Kaxiras (Uppsala University, Sweden)</i>	
Extending and Defending Attacks on Reset Operations in Quantum Computers .....	73
<i>Jerry Tan (Yale University, USA), Chuanqi Xu (Yale University, USA), Theodoros Trochatos (Yale University, USA), and Jakub Szefer (Yale University, USA)</i>	

## Session 3: Secure Execution Environments

SSE: Security Service Engines to Scale Enclave Parallelism for System Interactive Applications .....	84
<i>Jared Nye (University of Connecticut, USA), Usman Ali (University of Connecticut, USA), and Omer Khan (University of Connecticut, USA)</i>	
Trusted Execution Environments in Embedded and IoT Systems: A CactiLab Perspective .....	96
<i>Ziming Zhao (University at Buffalo, USA), Md Armanuzzaman (University at Buffalo, USA), Xi Tan (University at Buffalo, USA), and Zheyuan Ma (University at Buffalo, USA)</i>	
SoK: A Comparison Study of Arm TrustZone and CCA .....	107
<i>Haoyang Huang (Southern University of Science and Technology, China), Fengwei Zhang (Southern University of Science and Technology, China), Shoumeng Yan (Ant Group, China), Tao Wei (Ant Group, China), and Zhengyu He (Ant Group, China)</i>	

## Session 4: Crypto Hardware and Accelerations

CiFHER: A Chiplet-Based FHE Accelerator with a Resizable Structure .....	119
<i>Sangpyo Kim (Seoul National University, Republic of Korea), Jongmin Kim (Seoul National University, Republic of Korea), Jaeyoung Choi (Seoul National University, Republic of Korea), and Jung Ho Ahn (Seoul National University, Republic of Korea)</i>	
LOaPP: Improving the Performance of Persistent Memory Objects via Low-Overhead at-Rest PMO Protection .....	131
<i>Derrick Greenspan (n/a), Naveed Ul Mustafa (n/a), Andres Delgado (n/a), Connor Bramham (n/a), Christopher Prats (n/a), Samu Wallace (n/a), Mark Heinrich (n/a), and Yan Solihin (n/a)</i>	

SoK: Opportunities for Accelerating Multi-Party Computation via Trusted Hardware .....	143
<i>Tong Liu (Southern University of Science and Technology, China), Zhen Huang (Shanghai Jiao Tong University, China), Jiaao Li (Tsinghua University, China), Jianyu Niu (Southern University of Science and Technology, China), Guoxing Chen (Shanghai Jiao Tong University, China), and Yinqian Zhang (Southern University of Science and Technology, China)</i>	
Aggregate Encryption Individual Decryption for FPGA Bitstream Protection on Cloud .....	155
<i>Mukta Debnath (Indian Statistical Institute, India), Krishnendu Guha (University College Cork, Ireland), Debasri Saha (University of Calcutta, India), and Susmita Sur-Kolay (Indian Statistical Institute, India)</i>	
<b>Author Index .....</b>	<b>167</b>