

2025 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2025)

**Nanjing, China
19-21 December 2025**

IEEE Catalog Number:
ISBN:

CFP25F99-POD
979-8-3315-8925-7



Copyright © 2025, IEEE

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:	CFP25F99-POD
ISBN (Print-On-Demand):	979-8-3315-8925-7
ISBN (Online):	979-8-3315-8924-0

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

TABLE OF CONTENTS

BadHMP: Backdoor Attack Against Human Motion Prediction	1
<i>Chaohui Xu, Si Wang, Chip-Hong Chang</i>	
Leveraging Large Language Models for Secure Hardware Verification and Analysis	7
<i>Yifang Zhao, Weimin Fu, Yi-Xiang Hu, Shijie Li, Xiaolong Guo, Yier Jin</i>	
Fixbench-RTL: A Comprehensive Benchmark for Evaluating LLMs on RTL Debugging	11
<i>Shijie Li, Weimin Fu, Yifang Zhao, Xiaolong Guo, Yier Jin</i>	
Privacy-Preserving CNN Inference on FPGA Framework with High Throughput	17
<i>Qidong Chen, Yifan Yang, Wenpeng Zhao, Yijie Wang, Zhaojun Lu, Peng Xu, Jiliang Zhang</i>	
Split+Prune: Constructing Minimal Eviction Set under the LRU Replacement Policy	23
<i>Yi Han, Pengfei Qiu, Yihao Yang, Chunlu Wang, Dongsheng Wang, Jian Dong, Gang Qu</i>	
Lock+Umonitor+Umwait: Exposing the Security Risk of Lock Instruction in Achieving the Transient Execution Attack without Timer	29
<i>Yuzhang Duan, Pengfei Qiu, Chunlu Wang, Yihao Deng, Zhihao Zhang, Dongsheng Wang, Jiaji He, Gang Qu</i>	
A Unified Hardware Accelerator for Paillier and ElGamal with Masking and Improved Randomized Montgomery Ladder	35
<i>Jianfei Wang, Zichu Liu, Jia Hou, Yishuo Meng, Zhijie Lin, Huansheng Shi, Maoquan Cai, Chen Yang</i>	
Rethinking LLM Safety on Edge Devices: Unearthing Hidden Vulnerabilities through Power Stress	41
<i>Weimin Fu, Zelin Lu, Gang Qu, Xiaolong Guo</i>	
Modeling Fault Propagation for Model-Based Diagnosis as a MaxSAT Problem	47
<i>Huisi Zhou, Ning Kang, Wei Hu</i>	
FPGA-Accelerated SPHINCS+: An Area-Optimized and High-Throughput Design	53
<i>Yanfeng Bai, Bei Wang, Jiansheng Chen, Chenghua Wang, Yijun Cui, Weiqiang Liu</i>	
An Efficient Barrett Modular Multiplier Design for Zero-Knowledge Proof	59
<i>Jiahao Li, Qiang Liu, Ray C.C. Cheung, Zhaohui Guo</i>	
ARXPUF: A Modeling Attack Resilient Lightweight Strong PUF based on Add-Rotate-Xor	63
<i>Zhenzhe Chen, Weirong Dong, Kunyang Liu, Takashi Sato</i>	
Bug Hunting in the RISC-V SoC: The 1 st Integrated Circuit Security Challenge	69
<i>Lei Peng, Jiacheng Zhu, Qizhi Zhang, Shibo Tang, Xingxin Wang, Xinyu Zheng, Yaxuan Zhao, Aijiao Cui, Wei Hu, Jiaji He, Peng Fei Qiu</i>	
Adversarially Evasive Hardware Trojans through Approximate Designs	75
<i>Marwa Dhiaf, Halima Bouzidi, Ihsen Alouani</i>	
RejSCore: Rejection Sampling Core for Multivariate-based Public key Cryptography	79
<i>Malik Imran, Safiullah Khan, Zain Ul Abideen, Ciara Rafferty, Ayesha Khalid, Muhammad Rashid, Máire O'Neill</i>	

DASH-T: A Lightweight Countermeasure Based on Dynamic Address Shuffling and Temporal-hiding for Kyber’s PWM	85
<i>Jiaji He, Yucheng Fu, Jindi Kong, Pengfei Qiu, Mao Ye, Yiqiang Zhao</i>	
Evaluating Proposed Countermeasures for Power Analysis of Ring Oscillator PUFs	91
<i>James Moore, Jack Miskelly, Máire O’Neill, Chongyan Gu</i>	
A Quantitative Framework for Autocorrelation Analysis and Modeling Resistance Assessment of Physically Unclonable Functions	97
<i>Yuan Ma, Bi Wang, Chao Wang, Zhaohao Wang</i>	
SHAFI: Securing Hash-Based Post-Quantum Cryptography from Hardware Fault Injection Attacks	101
<i>Yanze Wu, Qian Wang, Md Tanvir Arafin</i>	
A Portable and Hybrid Verification Framework Using C and UVM for Secure RISC-V SoCs	105
<i>Muhammad Yasir Farooq, Haroon Waris, Chenghua Wang, Muhammad Usman Akram, Jiatong Tian Jiang Li, Weiqiang Liu</i>	
Flexible NTT Accelerator Design Framework for Scalable Lattice-Based Cryptosystems	111
<i>Yiqiang Zhao, Yanhui Song, Xintong Song, Qizhi Zhang, Yao Li, Jiaji He</i>	
PPA: Novel Page Prefetcher-Based Side-Channel Attacks	117
<i>Tengjiao Fu, Yu Jin, Dongsheng Wang, Shuwen Deng, Yun Chen</i>	
NNUF: Nearest Neighbor Union-Find Decoder for Quantum Error Correction	123
<i>Yuhang Gu, He Li</i>	
SACRED EYE: Secure Communication and Decentralized Monitoring for Swarm UAV Mission Completion	127
<i>Hugo Le Dirach, Amin Rezaei</i>	
An Auto-profiling Side-Channel Attack against NTT Hardware Implementations	133
<i>Yiting Wang, Zelin Lu, Gang Qu, Md Tanvir Arafin</i>	