2023 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2023)

Tianjin, China
13-15 December 2023

IEEE Catalog Number: CFP23F99-POD
ISBN: 979-8-3503-4100-3

****** 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:	CFP23F99-POD
ISBN (Print-On-Demand):	979-8-3503-4100-3
ISBN (Online):	979-8-3503-4099-0

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

Hardware Security of Digital Image Filter IP Cores Against Piracy Using IP Seller's Fingerprint Encrypted Amino Acid Biometric Sample 1
Anirban Sengupta, Rahul Chaurasia, Aditya Anshul

TrustSoC: Light and Efficient Heterogeneous SoC Architecture, Secure-By-Design 7
Raphaële Milan, Lilian Bossuet, Loïc Lagadec, Carlos Andres Lara-Nino, Brice Colombier

Fault Analysis on AES and SM4 Through Automatic Property Extraction and Checking 13
Xingxin Wang, Xinxin Wang, Chaoxuan Yuan, Wei Hu

Overtake: Achieving Meltdown-Type Attacks with One Instruction 18
Yu Jin, Pengfei Qiu, Chunlu Wang, Yihao Yang, Dongsheng Wang, Xiaoyong Li, Qian Wang, Gang Qu

Tamper Resistant Design of Convolutional Neural Network Hardware Accelerator 24
Haosen Yu, Peiyao Sun, Basel Halak, Karthik Shanthakumar, Tomasz Kazmierski

Emulating Covert Data Transmission on Heterogeneous SoCs 29
Lilian Bossuet, Carlos Andres Lara-Nino

AHD-LAM: A New Mitigation Method Against Voltage-Drop Attacks in Multi-Tenant FPGAs 35
Mashrafi Alam Kajol, Sandeep Sunkavilli, Qiaoyan Yu

A Lightweight and Machine-Learning-Resistant PUF Framework Based on Nonlinear Structure and Obfuscating Challenges 41
Tianming Ni, Fei Li, Qingsong Peng, Senling Wang, Xiaoqing Wen

DDQ-APUF: A Highly Reliable Arbiter PUF Using Delay Difference Quantization 47
Xue Mei, Guangyang Zhang, Chongyan Gu, Yao Wang

NNLeak: An AI-Oriented DNN Model Extraction Attack Through Multi-Stage Side Channel Analysis 51
Ya Gao, Haocheng Ma, Mingkai Yan, Jiaji He, Yiqiang Zhao, Yier Jin

A Comparative Analysis Between Karatsuba, Toom-Cook and NTT Multiplier for Polynomial Multiplication in NTRU on FPGA 57
Harish Prasad Allam, Suraj Mandal, Debapriya Basu Roy

Processor Based Intrinsic PUF Design for Approximate Computing: Faith Or Reality? 63
Aditya Japa, Jiliang Zhang, Weiqiang Liu, Chongyan Gu

A Hybrid Neural Network for Simultaneous Multi-Attack Detection in Sensor Networks 69
Nishanth Chennagouni, Mohammad Monjur, Wei Lu, Qiaoyan Yu

LLM4SecHW: Leveraging Domain-Specific Large Language Model for Hardware Debugging 75
Weimin Fu, Kaichen Yang, Raj Gautam Dutta, Xiaolong Guo, Gang Qu

A Comparison of One-Class and Two-Class Models for Ransomware Detection Via Low-Level Hardware Information 81
Chutitep Woralert, Chen Liu, Zander Blasingame, Zhiliu Yang

HeisenTrojans: They Are Not There Until They Are Triggered 87
Akshita Reddy Mavurapu, Haoqi Shan, Xiaolong Guo, Orlando Arias, Dean Sullivan

When Memory Mappings Attack: On the (Mis)use of the ARM Cortex-M FPB Unit 94
Haoqi Shan, Dean Sullivan, Orlando Arias

A Lightweight Authentication Scheme with PE-Based Unclonable Label 100
Renchao Li, Zhen Weng, Aijiao Cui, Gang Qu

A Compact Weak PUF Circuit Based on Random Process Deviations of Amplifier Chain 106
Pengjun Wang, Yuanfeng Xie, Gang Li

DF-TEE: Trusted Execution Environment for Disaggregated Multi-FPGA Cloud Systems 111
Ke Xia, Sheng Wei

Author Index