

2022 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2022)

**Singapore
14 – 16 December 2022**



**IEEE Catalog Number: CFP22F99-POD
ISBN: 978-1-6654-6115-3**

**Copyright © 2022 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:	CFP22F99-POD
ISBN (Print-On-Demand):	978-1-6654-6115-3
ISBN (Online):	978-1-6654-6114-6

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

TABLE OF CONTENTS

Vulnerable PQC Against Side Channel Analysis - A Case Study on Kyber	1
<i>Haocheng Ma, Shijian Pan, Ya Gao, Jiayi He, Yiqiang Zhao, Yier Jin</i>	
A Lightweight M_TRNG Design Based on MUX Cell Entropy Using Multiphase Sampling	7
<i>Liang Yao, Huaguo Liang, Hong Zhang, Tianming Ni, Maoxiang Yi, Yingchun Lu</i>	
A Machine Learning Based Automatic Hardware Trojan Attack Space Exploration and Benchmarking Framework	11
<i>Jonathan Cruz, Pravin Gaikwad, Abhishek Nair, Prabuddha Chakraborty, Swarup Bhunia</i>	
A Novel Cross-Platform Physically Unclonable Function for Emerging FPGA-Based IoT Devices.....	17
<i>Dipnarayan Das, Sourav Roy, Mahabub Hasan Mahalat, Bibhash Sen</i>	
A Novel Machine Learning Attack Resistant APUF with Dual-Edge Acquisition	21
<i>Hui Li, Gang Li, Pengjun Wang, Xilong Shao</i>	
A Structural and SAT Analysis of SANSCrypt.....	25
<i>James Geist, Shaojie Zhang, Yier Jin, Travis Meade</i>	
An Instruction-Configurable Post-Quantum Cryptographic Processor Towards NTRU	31
<i>Shuo Yang, Dongsheng Liu, Ang Hu, Aobo Li, Jiaming Zhang, Xiang Li, Jiahao Lu, Changwen Mo</i>	
Analysis of Hardware Trojan Resilience Enabled Through Logic Locking	37
<i>Jonathan Cruz, Pravin Gaikwad, Swarup Bhunia</i>	
EISec: Exhaustive Information Flow Security of Hardware Intellectual Property Utilizing Symbolic Execution.....	43
<i>Farhaan Fowze, Muhtadi Choudhury, Domenic Forte</i>	
EXERT: EXhaustive IntEgRiTy Analysis for Information Flow Security.....	49
<i>Jiaming Wu, Farhaan Fowze, Domenic Forte</i>	
FUNDAE: Fault Template Attack on SUNDAE-GIFT AEAD Scheme	55
<i>Rajat Sadhukhan, Anirban Chakraborty, Debdeep Mukhopadhyay</i>	
Fundamental Study of Adversarial Examples Created by Fault Injection Attack on Image Sensor Interface.....	61
<i>Tatsuya Oyama, Kota Yoshida, Shunsuke Okura, Takeshi Fujino</i>	
gr-tempest: An Open-Source GNU Radio Implementation of TEMPEST	67
<i>Federico Larroca, Pablo Bertrand, Felipe Carrau, Victoria Severi</i>	
HARD-Lite: A Lightweight Hardware Anomaly Realtime Detection Framework Targeting Ransomware	73
<i>Chutitep Woralert, Chen Liu, Zander Blasingame</i>	
Incremental Linear Regression Attack.....	79
<i>Juncheng Chen, Jun-Sheng Ng, Nay Aung Kyaw, Zhili Zou, Kwen-Siong Chong, Zhiping Lin, Bah-Hwee Gwee</i>	
iPROBE-O: FIB-aware Place and Route for Probing Protection Using Orthogonal Shields	83
<i>Minyan Gao, Domenic Forte</i>	

KEATON: Assertion-Guided Attack on Combinational and Sequential Locking Without Scan Access.....	89
<i>Mahmudul Hasan, Tamzidul Hoque</i>	
LSB-Reused Protection Technique in Secure SAR ADC Against Power Side-Channel Attack.....	95
<i>Lele Fang, Jiahao Liu, Yan Zhu, Chi-Hang Chan, Rui Paulo Martins</i>	
MRCO: A Multi-Ring Convergence Oscillator-Based High-Efficiency True Random Number Generator.....	101
<i>Tianming Ni, Qingsong Peng, Jingchang Bian, Liang Yao, Zhengfeng Huang, Aibin Yan, Xiaoqing Wen</i>	
On the Limitations of Logic Locking the Approximate Circuits.....	107
<i>Kartik Nayak, Devanshi Upadhyaya, Francesco Regazzoni, Ilia Polian</i>	
PMU-Spill: Performance Monitor Unit Counters Leak Secrets in Transient Executions.....	113
<i>Pengfei Qiu, Qiang Gao, Dongsheng Wang, Yongqiang Lyu, Chang Liu, Xiaoyong Li, Chunlu Wang, Gang Qu</i>	

Author Index