

2025 2nd International Conference On Cryptography And Information Security (VCRIS 2025)

**Hanoi, Vietnam
30-31 October 2025**

IEEE Catalog Number:
ISBN:

CFP25ZZ7-POD
979-8-3315-6688-3



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:	CFP25ZZ7-POD
ISBN (Print-On-Demand):	979-8-3315-6688-3
ISBN (Online):	979-8-3315-6687-6

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

TABLE OF CONTENTS

Turbo Codes-based Physical Layer Security Method Against Passive Eavesdropping Attacks For MIMO Wireless Communication Systems	1
<i>Dinh Van Linh, Hoang Thi Phuong Thao, Vu Van Yem</i>	
A Multimodal Model for Detecting Vietnamese Toxic News Using Semi-supervised Learning	7
<i>Ngoc An Le, Xuan Dau Hoang, Thi Thu Trang Ninh</i>	
Stochastic Updating in Federated Learning	13
<i>Quang Minh Tran, Tuan Cuong Nguyen, Hong Ngoc Tran</i>	
Hardening DLT-Daemon against TOCTOU Vulnerabilities: A Study on Atomic Mutex Locking for Critical State Resilience	17
<i>Minh Luu Quang, Ngoc Hong Tran</i>	
A Hybrid Balancing Method for IDS Datasets Using CTGAN + K-Means	23
<i>Thanh Tra Ung, Cong Thanh Nguyen, Tan Duy Le, Duy Trung Pham, Thu Lam Bui</i>	
A Novel Approach for Aggregation of Teacher Ensembles with Secure Multi-Party Computation	29
<i>Anh-Tu Tran, Thi Hong Ha Nguyen</i>	
Optimizing Secure Network Coding: A Comparative Analysis of Hybrid Cryptosystems with Relay-Enhanced Topology	37
<i>Phetphachan Thammasith, Trung Hieu Nguyen, Hieu Minh Nguyen</i>	
DefacementFusion: A Robust Multi-Modal Defacement Detection	44
<i>Phan Hai Dang, Nguyen Trong Hung, Huynh Ngoc Khanh, Duc-Tho Mai</i>	
Side-Channel Attack on XOR Operation in the First Round of AES Implementation on the STM32 Microcontroller Board	50
<i>Ha Hai Pham, Duc Chinh Bui, Ngoc Vinh Hao Nguyen, Van Hai Le, Quoc Tien Dinh, Viet Manh Nguyen</i>	
CRYSTALS-Kyber KEM Decapsulation with Single-Point Pseudo-Random Cache Flushing	54
<i>Stephanie Shinn, Sena Hounsinnou</i>	
Q-SafeAV: Quantum-enabled Secure Intra-Sensor Communication Framework for AVs	60
<i>Rajan Datt, Dhiraj Singh, Ayush Goyal, Tejas Singh, Rajesh Gupta, Sudeep Tanwar, Anand Nayyar</i>	
BLOCKTAIL: A Large-Size and Efficiently Implemented Bit-Oriented Design for Block Ciphers and Permutations	67
<i>Hoang Dinh Linh, Nguyen Van Long, Luong Tran Thi</i>	
A Model of Quantum Tunneling with Knots and Braid Operators	71
<i>Phuong-Nam Nguyen</i>	
Robust Image Watermarking Algorithm Integrating QR and Singular Value Decomposition in the Discrete Wavelet Transform Domain	75
<i>Nguyen Thanh Hai, Ta Minh Thanh</i>	
Implementation of the BHT quantum algorithm for finding collisions of a lightweight hash function on IBM “Sherbrooke” via Qiskit	81
<i>Nghi Nguyen Van, Minh Thang Vu, Hanh Tran Thi, Nam Hai Ngo, Ba Linh Vu, Van Duan Nguyen</i>	

Intrusion Detection in IoT Networks using a Hybrid Quantum-Classical Graph Neural Network	87
<i>Trong Binh Hoang, Dinh Van Linh</i>	
Threshold-Based Entity Authentication for PKCS#11: A Cryptographic Protocol Using Shamir's Secret Sharing	93
<i>Hoang Van Thuc, Hoang Sy Tuong</i>	
Detecting Source Code Vulnerabilities Across Programming Languages Using Traditional Machine Learning: A Transfer Learning Based and Language Independent Approach	99
<i>Tuan Nguyen Kim, Tho Hoang Duc, Nin Ho Le Viet, Duc Tong Minh</i>	
Post-Quantum Signature Algorithm On Finite Matrix Algebras, Using Three Hidden Groups	103
<i>Khanh-Linh Dinh, Long-Giang Nguyen, Hieu-Minh Nguyen, Thi-Bac Do, Alexandr A. Moldovyan Dmitriy N. Moldovyan, Anna A. Kostina</i>	
Android Malware Classification Based on Graph Features and Graph Neural Networks	111
<i>Le Duc Thuan, Nguyen Van Thanh, Pham Van Huong</i>	
Reversible data hiding in encrypted images using two-pass improved pixel value ordering on high-bit segments	117
<i>Ngoc-Van-Khanh Duong, Thai-Son Nguyen</i>	
UniFuzz: A Unified Fuzzing Framework for Smart Contract Vulnerability Detection with LLMs and Audit Reports	121
<i>Le Quoc Ngo, Tran Tien Nhat, Nguyen Huu Quyen, Van-Hau Pham, Phan The Duy</i>	
Adversarial Noise Injection for Side-Channel Resistance	127
<i>Tran Ngoc Quy, Nguyen Nhu Chien, Lê Thi Ninh</i>	
RTL Design and Implementation of the TWINE-80 Lightweight Block Cipher	133
<i>Linh Nguyen Thi Thuy, Thanh-Ngoc Nguyen, Bui Duc Trinh, Duc-Tho Mai</i>	
DBA: A Novel Diffusion-Based Method for Adversarial Defense via Image Restoration	139
<i>Pham Duy Trung, Truong Phi Ho, Do Duy Khanh, Nguyen Nhat Hai</i>	
Improved Neural Distinguisher for PRESENT-80 using Inception and Efficient Channel Attention in Related-Key Multi-Pair Setting	146
<i>Thanh-Phong Nguyen, Nguyen Tan Cam, Van-Than Huynh, Tan Nguyen, Hieu-Minh Nguyen</i>	
A Method For Dynamically Modifying Component Transformations in The AES Block Cipher Applied To Image Data Encryption	154
<i>Phuong Truong Minh, Thuc Hoang Van, Luong Tran Thi, Duyet Bui Nhat</i>	
Blockchain-Integrated 5G Authentication: A ProVerif Formal Analysis Approach	160
<i>Tran Thi Nga, Nguyen Thanh Tung, Nguyen Duc Cong, Dinh Van Hung, Duc-Tho Mai</i>	
Multimodal Fusion of Behavior Graphs and API Sequences for Ransomware Detection	166
<i>Dinh Le Thanh Cong, Ho Hoang Diep, Nghi Hoang Khoa, Do Thi Thu Hien, Phan The Duy</i>	
A PQC Engine You Didn't Know You Had: Exploring DSP for Cryptographic Acceleration	172
<i>Florian Caullery</i>	
Reliability and Security Analysis of Power Beacon Based Half-Duplex Relaying System With Hardware Impairments	178
<i>Dang The Hung, Nguyen Hieu Minh</i>	

VeriBridge: Real-Time Cross-Chain Bridge Attack Detection through Static-Informed Graph Anomaly Learning	184
<i>Tuan-Dung Tran, Dinh Khang Nguyen, Quang Trung Do, Van-Hau Pham</i>	
Cross-System Few-shot Log Anomaly Detection with Transformer-based Supervised Autoencoder and Data Augmentation	190
<i>Manh Tuan Nguyen, Trang Dang Le Dinh, Van Loi Cao</i>	
FPGA Implementation of Kuznyechik Block Cipher with Improved Resource Efficiency	196
<i>Ba-Anh Dao, Dinh-Hung Le, Ngoc-Quynh Nguyen</i>	
Multi-Layer Defense for AI-powered IDS: Ensemble Adversarial Training and Explainable Resilience to Evasion Attacks	201
<i>Hanh P. Du, Minh Q. Tran, Tuyen T. Nguyen, Hoa N. Nguyen</i>	
Multi-Scale Attention-Enhanced Block-Based Steganography: A Comprehensive Analysis of Capacity-Quality Trade-offs	207
<i>Ngoc-Giau Pham, Khac-Hoang Nguyen, Hong-Ngoc Tran, Phuoc-Hung Vo</i>	
Novel Blind Colour Image Watermarking Technique Using Schur Decomposition	213
<i>Pham Thi Yen, Ta Minh Thanh, Nguyen Hieu Minh</i>	
Beyond Robustness: On the Unforgeability Trade-offs in Statistical DNN Watermarking	219
<i>Phuong-Dai Bui, Tuan-Dung Tran</i>	