

2024 1st International Conference on Cryptography and Information Security (VCRIS 2024)

**Hanoi, Vietnam
3-4 December 2024**



**IEEE Catalog Number: CFP24ZZ7-POD
ISBN: 979-8-3315-2995-6**

**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:	CFP24ZZ7-POD
ISBN (Print-On-Demand):	979-8-3315-2995-6
ISBN (Online):	979-8-3315-2994-9

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

	Pages
Keynotes	
Exposing Network Vulnerabilities: Security Insights from Tor, VoWiFi, and Cellular Networks <i>Edgar Weippl</i>	i
Secure implementation of Post-Quantum Cryptography <i>Sylvain Guilley</i>	ii
SOLMAE: Faster and simpler quantum-safe signature based on NTRU-lattices <i>Kwangjo Kim</i>	iii
A comprehensive view of the malware ecosystem is essential <i>Jean-Yves Marion</i>	iv
Invited Speaker	
MKV: A New Block Cipher of Vietnam for the Post-Quantum Cryptography Transition <i>Nguyen Bui Cuong</i>	v
Cryptography Session 1	
Short Lee-metric Code-based Signature <i>Chik How Tan and Theo Fanuela Prabowo</i>	1
Dimension Reduction Attack on Noncommutative Group Ring NTRU over the Dihedral Group <i>Vikas Kumar, Ali Raya, Aditi Kar Gangopadhyay and Sugata Gangopadhyay</i>	7
Resource-Efficient 4x4 S-boxes Using Chaotic Map <i>Phuc-Phan Duong, Ba-Anh Dao, Thai-Ha Tran, Trong-Hung Nguyen, Trong-Thuc Hoang and Cong-Kha Pham</i>	13
On Multi-Key FuncCPA Secure Encryption Schemes <i>Eri Nakajima, Keisuke Hara and Kyosuke Yamashita</i>	19
Information Security Session 1	
A New Method to Improve the CNN Configuration for IoT Attack Detection Problem based on the Genetic Algorithm and Multi-Objective Approach <i>Le Thi Hong Van, Le Duc Thuan, Pham Van Huong and Nguyen Hieu Minh</i>	25
An IoT Security Attack Classification Solution on the Perception Layer Using Shallow Machine Learning <i>Duc-Tho Mai, Lam-Tra Nguyen, Nga Tran Thi, Duc-Cong Nguyen and Thanh-Nam Pham</i>	34
AWDLID: Augmented WGAN and Deep Learning for Improved Intrusion Detection <i>Hoang V. Vo, Hanh P. Du and Hoa N. Nguyen</i>	40
Cryptography Session 2	
A simple and low-cost quantum random number generator based on coherent states <i>Phuc La Huu and Kien Vu Van</i>	46
A Compact SHA3 Implementation for Post-quantum Cryptography <i>Trong-Hung Nguyen, Duc-Thuan Dam, Phuc-Phan Duong, Cong-Kha Pham and Trong-Thuc Hoang</i>	50
Secure network coding based on the integer factorization problem <i>Phetphachan Thammassith, Trung Hieu Nguyen and Hieu Minh Nguyen</i>	55

Crypto-coding method based on the components of Turbo code <i>Dinh Van Linh, Nguyen Tuan Anh, Dang Thi Thu Huong, Hoang Thi Phuong Thao and Vu Van Yem</i>	61
A "Kuznyechik" block cipher accelerator for RISC-V System-on-Chip <i>Ba Anh Dao, Ngoc-Quynh Nguyen and Chung-Tien Nguyen</i>	67
Information Security Session 2	
Employing a CNN detector to identify AI-generated images and against attacks on AI systems <i>Phi-Ho Truong, Tien-Dung Nguyen, Xuan-Hung Truong, Nhat-Hai Nguyen and Duy-Trung Pham</i>	72
Blockchain-Powered e-Wallet: Enhancing Security and Fraud Detection in Online Payments <i>Dong Bui-Huu, Tan Le-Nhat and Khuong Nguyen-An</i>	78
A Deep Metric Learning Approach for Cyber Reconnaissance Detection <i>Van Quan Nguyen, Long Thanh Ngo, Viet Hung Nguyen, Le Minh Nguyen and Nhien-An Le-Khac</i>	84
High-Capacity RDH in Encrypted Images Based on Interpolation Mechanism <i>Hoang-Nam Tram and Thai-Son Nguyen</i>	91
Spatial Vision Transformer: A Novel Approach to Deepfake Video Detection <i>Pham Minh Thuan, Bui Thu Lam and Pham Duy Trung</i>	97
Security, Privacy, and Ethical Challenges of Artificial Intelligence in Large Language Model Scope: A Comprehensive Survey <i>Tuyen T. Nguyen, Huyen Vu Thi Thanh and Hoa N. Nguyen</i>	103
Cryptography Session 3	
Proposed Novel Architectures for Constructing Lightweight Dynamic S-Boxes <i>Quang-Huy Tran, Hieu-Minh Nguyen, Thi-Bac Do, Van-Quyen Phung, Tuan-Dat Duong and Phuc-Phan Duong</i>	109
On the Mathematical Aspects of Cryptographic Randomness Tests using Discrete Fourier Transform <i>Linh Hoang Dinh, Luong Tran Thi and Long Nguyen Van</i>	116
Recycling of Grain-v1 for faster communication <i>Santu Pal</i>	122
Side-Channel Attack on Implementation of AES T-Box Encryption on STM32 Microcontroller Board <i>Ha Hai Pham, Duc Chinh Bui, Ngoc Vinh Hao Nguyen, Van Hai Le, Quoc Tien Dinh and Van-Phuc Hoang</i>	128
Information Security Session 3	
Novel Blind Colour Image Watermarking Technique Using Cholesky Decomposition <i>Yen Pham, Thanh Minh Ta and Minh Hieu Nguyen</i>	134
I-SteganoGAN: Comprehensive Enhancement of Steganographic Models for Robust Digital Communication Security <i>Ngoc-Giau Pham, Anh-Khoa Ngo Dinh, Phuoc-Hung Vo and Hong-Ngoc Tran</i>	140
A Novel Deep Learning Approach with Magnet Loss Optimization for Website Attack Detection <i>Dai Duong Tang, Van Quan Nguyen, Viet Hung Nguyen, Thanh Cong Nguyen and Nathan Shone</i>	146

Transformer Models for Prompt Jailbreak Attack Detection in AI Assistant Systems Optimizing	152
<i>Anh-Tien Le and Van Huong Pham</i>	

Session for Short papers

Secure Coordinate Rotation in Embedded Systems Using Homomorphic Encryption: Implementation and Evaluation on the AI-Saqr Platform	156
<i>Yashrajsinh Parmar, Florian Caullery and Sonali Kale</i>	
Defining High-Dimensional Non-Commutative Algebras as Carriers for Post-Quantum Digital Signature Algorithms	162
<i>Linh Khanh Dinh, Bac Thi Do, Nguyen Long Giang, Alexandr A. Moldovyan, Dmitriy N. Moldovyan and Anna A. Kostina</i>	
A Multi-objective Approach to Improve Hyper-parameters of CNN for Network Intrusion Detection Problem	167
<i>Pham Thanh Cong, Pham Van Huong and Le Quang Minh</i>	
ASAF: AI-powered Static Analysis Framework for Webshell Detection	175
<i>Ha V. Le, Hieu T. Hoang, On V. Phung and Hoa N. Nguyen</i>	