

2025 9th International Conference on Cryptography, Security and Privacy (CSP 2025)

**Okinawa, Japan
26-28 April 2025**



**IEEE Catalog Number: CFP25Z50-POD
ISBN: 979-8-3315-2470-8**

**Copyright © 2025 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:	CFP25Z50-POD
ISBN (Print-On-Demand):	979-8-3315-2470-8
ISBN (Online):	979-8-3315-2469-2

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

2025 9th International Conference on Cryptography, Security and Privacy (CSP) **CSP 2025**

Table of Contents

Preface	ix
Organizing Committee	x
Reviewers	xii

Modern Cryptography Theory and Encryption Technology

Cryptanalysis of an Effective Certificateless Aggregate Signcryption Scheme	1
<i>Moirangthem Rabindra Singh (National Institute of Technology Meghalaya, India) and Surmila Thokchom (National Institute of Technology Meghalaya, India)</i>	
Reducing the e-KYC File Searching Time in the Blockchain System using Searchable Symmetric Encryption and Turbulence Padded Chaotic Map	6
<i>Lalu Raynaldi Pratama Putra (Telkom University, Indonesia) and Ari Moesriami Barmaui (Telkom University, Indonesia)</i>	
Leveraging Open Source INTelligence (OSINT) for Cryptocurrency Crime Investigation using Tools and Techniques	12
<i>Byung Wan Suh (Fairsquarelab Co., Ltd., Korea) and Won-Woong Kim (Fairsquarelab Co., Ltd., Korea)</i>	
The Giant Footprint is the Smallest: Low-Footprint Decryption of Classic McEliece	17
<i>Cong Liu (Panasonic Corporation, Japan), Naoto Yanai (Panasonic Holdings Corporation, Japan), Naohisa Nishida (Panasonic Holdings Corporation, Japan), and Akira Maruko (Panasonic Holdings Corporation, Japan)</i>	
CSSM: A Combined Structure of SM4-Like Structure and MARS-Like Structure	22
<i>Zhengyi Dai (National University of Defense Technology, China) and Chao Li (National University of Defense Technology, China)</i>	
Enhancing Side-Channel Attack Resistance of Post-Quantum Cryptographic Algorithm CRYSTALS-Kyber using High-Order Chebyshev Filters	28
<i>Chung-Wei Kuo (Feng-Chia University, Taiwan), Wei-Chih Hong (Feng-Chia University, Taiwan), Yi-Kai Hsu (Feng-Chia University, Taiwan), and Yu-Yi Hong (Feng-Chia University, Taiwan)</i>	
Cryptography Based on 2D Ray Tracing	33
<i>Sneha Mohanty (University of Freiburg, Germany) and Christian Schindelbauer (University of Freiburg, Germany)</i>	

Optimizing Hybrid Cryptographic Frameworks for Secure Financial Data Transmission in Resource-Constrained Environments	41
<i>Paul Kobina Arhin Jnr (University of Cape Coast, Ghana), George Aggrey (University of Cape Coast, Ghana), Michael Asante (KNUST, Ghana), and Linda Otoo (University of Cape Coast, Ghana)</i>	

Information Security and Privacy Protection

A Blockchain-Enhanced Reversible Watermarking Framework for End-to-End Data Traceability in Federated Learning Systems	46
<i>Reda Bellafqira (IMT Atlantique, France), Chloé Berton (IMT Atlantique, France), and Gouenou Coatrieux (IMT Atlantique, France)</i>	
Privacy-Preserved PQC-Based UCSSO in Telemedicine Systems	53
<i>Tzu-Wei Lin (Feng Chia University, Taiwan) and Chieh-Jung Yu (Feng Chia University, Taiwan)</i>	
A Blockchain-Integrated IoT System Leveraging Hyperledger Fabric	58
<i>Yiming Sun (New York Institute of Technology, Canada), Zakaria Alomari (New York Institute of Technology, Canada), Rong Lian (New York Institute of Technology, Canada), and Jianchao Lai (New York Institute of Technology, Canada)</i>	
Research on Integrity Measurement of Trusted Access for Cloud Manufacturing Equipment Terminals	64
<i>Wenbo Wei (Taiyuan University of Science and Technology, China), Mengyuan Li (Taiyuan University of Science and Technology, China), and Yin Zhang Guo (Taiyuan University of Science and Technology, China)</i>	
Further Attacks on the Micali-Schnorr Pseudorandom Generator	72
<i>Anders Mah (University of New South Wales, Australia), Liam Heng (University of New South Wales, Australia), Cameron McGowan (University of New South Wales, Australia), James Liu (University of New South Wales, Australia), and Amy Tian (University of New South Wales, Australia)</i>	
Electromagnetic Side-Channel Analysis of PRESENT Lightweight Cipher	77
<i>Nilupulee A. Gunathilake (Edinburgh Napier University, UK), Owen Lo (Edinburgh Napier University, UK), William J. Buchanan (Edinburgh Napier University, UK), and Ahmed Al-Dubai (Edinburgh Napier University, UK)</i>	
Defending Against Gaussian Process Membership Inference Attack	82
<i>Rashedul Islam (University of The Ryukyus, Japan), Jannatul Ferdous Akhi (University of The Ryukyus, Japan), and Takayuki Nakachi (University of The Ryukyus, Japan)</i>	

Network Intrusion Detection and Defense

Interrupt Trace Fusion for Enhanced Website Fingerprinting Attacks under Defensive Mechanisms	87
<i>Yefeng Lv (Shanghai Maritime University, China), Jiajia Jiao (Shanghai Maritime University, China), Hong Yang (Shanghai Maritime University, China), and Ran Wen (Shanghai Maritime University, China)</i>	

Evaluating Boundary Restriction Methods Against Hardware Transient Faults on Website Fingerprinting Attacks	94
<i>Chaoyue Ren (Shanghai Maritime University, China), Yixu Yu (Shanghai Maritime University, China), Ran Wen (Shanghai Maritime University, China), and Jiajia Jiao (Shanghai Maritime University, China)</i>	
Optimization of Class Imbalance Techniques in Machine Learning Models for Network Intrusion Detection	102
<i>Huijie Xie (New York Institute of Technology, Canada), Yunlong Shao (New York Institute of Technology, Canada), Zhida Li (New York Institute of Technology, Canada), Zakaria Alomari (New York Institute of Technology, Canada), and Adetokunbo Makanju (New York Institute of Technology, Canada)</i>	
Optimizing Real-Time Network Intrusion Detection using a Refined Data Filtering Method	107
<i>Zhida Li (New York Institute of Technology, Canada), Chunyang Zhu (New York Institute of Technology, Canada), Changlin Chu (New York Institute of Technology, Canada), Cong He (New York Institute of Technology, Canada), Yunlong Shao (New York Institute of Technology, Canada), Zakaria Alomari (New York Institute of Technology, Canada), and Adetokunbo Makanju (New York Institute of Technology, Canada)</i>	
Mitigating Server-Side Request Forgery (SSRF) Attacks: An Empirical Analysis of Deep Learning-Based Approaches	112
<i>Jacqueline Mukamisha (Carnegie Mellon University, Rwanda), Aline Iradukunda (Carnegie Mellon University, Rwanda), Elyse Manzi (Carnegie Mellon University, Rwanda), and Jema Ndibwile (Carnegie Mellon University, Rwanda)</i>	
Investigating Sample Selection Methods for Fast and Precise Feature Attribution Explanations in Intrusion Detection	120
<i>Elyes Manai (Laval University, Canada), Mohamed Mejri (Laval University, Canada), and Jaouhar Fattahi (Laval University, Canada)</i>	
Edge-Based Machine Learning Models in IoT Devices for Improved Anomaly and Intrusion Detection	127
<i>Theodore Kindong (Linköping University, Sweden) and Sarfraz Iqbal (Linnaeus University, Sweden)</i>	
Reusable Attack Tree Patterns using Common Attack Pattern Enumeration and Classification	132
<i>Masaki Oya (Institute of Information Security, Japan), Keita Yamamoto (Institute of Information Security, Japan), Masaki Hashimoto (Kagawa University, Japan), and Takao Okubo (Institute of Information Security, Japan)</i>	
Integrating Tree Structures with the MITRE ATT&CK Framework for APT Detection	139
<i>Wen-Tsung Tsai (National Defense University, Taiwan), Jia-Ning Luo (National Defense University, Taiwan), and Chao-Lung Chou (Feng Chia University, Taiwan)</i>	
Towards Systemic IT Security. Introducing a Holistic Conceptual Framework for a Society-Centered Perspective Connecting IT and Cyber Security	144
<i>Rainer Rehak (Weizenbaum Institute for the Networked Society, Germany)</i>	

Advanced Information Theory and Security Technology

Dimensionality Reduction for Enhancing Malware Classification Accuracy in Portable Executable Files	156
<i>Mathew Nicho (Rabdan Academy, Australia), Kushal K. Rahatkar (Robert Gordon University, United Kingdom), and Christopher D. McDermott (Robert Gordon University, United Kingdom)</i>	
Commitment Based Identity-Based Homomorphic Signatures for E-Document	163
<i>Apurva Kiran Vangujar (University College Cork, Ireland), Buwana Ganesh (University College Cork, Ireland), and Paolo Palmieri (University College Cork, Ireland)</i>	
SRAM PUFs for Device Authentication on Resource-Constrained Systems	169
<i>Manuel Penz (University of Applied Sciences Upper Austria, Austria), Martina Zeinzinger (University of Applied Sciences Upper Austria, Austria), Michael Kargl (University of Applied Sciences Upper Austria, Austria), Florian Eibensteiner (University of Applied Sciences Upper Austria, Austria), Phillip Petz (University of Applied Sciences Upper Austria, Austria), and Josef Langer (University of Applied Sciences Upper Austria, Austria)</i>	
Strengthening LoRaWAN Security Protocol Against Replay Attack Combined with RF Jamming Technique using Time Differential Privacy	177
<i>Daffa Tsany Rahmantyo (Telkom University, Indonesia), Ari Moesriami Barmawi (Telkom University, Indonesia), and Farah Afianti (Telkom University, Indonesia)</i>	
Shift-Left Security: Integrating Security in the Initial Phase of the DevOps Methodology	182
<i>Mathew Nicho (Rabdan Academy, Australia), Israel Effiong (Robert Gordon University, United Kingdom), and Christopher D. McDermott (Robert Gordon University, United Kingdom)</i>	
Analysis on Rolling Re-Pseudonymization without Accessing Plaintext Data for Distributed Secure Information Discovery	192
<i>Sascha Peitzsch (Fraunhofer FOKUS, Germany), Hannes Restel (Fraunhofer FOKUS, Germany), and Ulrich Meissen (Fraunhofer FOKUS, Germany)</i>	
Author Index	201