

# **2024 19th Asia Joint Conference on Information Security (AsiaJCIS 2024)**

**Tainan, Taiwan  
13-14 August 2024**



**IEEE Catalog Number: CFP2433T-POD  
ISBN: 979-8-3503-8015-6**

**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:	CFP2433T-POD
ISBN (Print-On-Demand):	979-8-3503-8015-6
ISBN (Online):	979-8-3503-8014-9
ISSN:	2374-0205

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2024 19th Asia Joint Conference on Information Security (AsiaJCIS) **AsiaJCIS 2024**

## Table of Contents

Message from the General Co-Chairs .....	ix
Message from the Program Co-Chairs .....	x
Organizing Committee .....	xi
Technical Program Committee .....	xii
Steering Committee .....	xiv
Reviewers .....	xv
Sponsors and Supporters .....	xvii

## Cryptography

Bit-Based MILP Modelling of Non-Bit-Permutation Linear Layers for Linear Cryptanalysis .....	1
<i>Abhilash Das (Indian Institute of Technology Jammu, India)</i>	
Cryptanalysis of PiLike: An Impersonation Attack on the Lightweight Identity-Based Authenticated Key Exchange Protocol Using Bi-ISIS .....	9
<i>Hao-Yi Hsu (National Chengchi University, Taiwan), Hsin-Yi Lin (National Chengchi University, Taiwan), Raylin Tso (National Chengchi University, Taiwan), Tao-Hsiang Chang (National Chengchi University, Taiwan), and Jen-Chieh Hsu (National Chengchi University, Taiwan)</i>	
A Study of Fully Homomorphic Encryption with Evaluation Control .....	17
<i>Kenneth Ong Kuan Phing (National Taiwan Normal University, Taiwan), Bo Yu Chen (National Taiwan Normal University, Taiwan), Po Wen Chi (National Taiwan Normal University, Taiwan), and Chao Wang (National Taiwan Normal University, Taiwan)</i>	
Consideration on Defining Field for Efficient Ring-LWE .....	25
<i>Rintaro Yamada (Osaka University, Japan), Shinya Okumura (Osaka University, Japan), and Atsuko Miyaji (Osaka University, Japan)</i>	
ID-Based Traitor Tracing with Relaxed Black-Box Setting for Group-Based Applications .....	33
<i>Yi-Fan Tseng (National Chengchi University, Taiwan), Raylin Tso (National Chengchi University, Taiwan), Shi-Sheng Sun (National Chengchi University, Taiwan), Zi-Yuan Liu (National Chengchi University, Taiwan), and You-Qian Chen (National Chengchi University, Taiwan)</i>	

## System Security

An Identity Management System using Group Signatures with Message-Dependent Opening .....	40
<i>Yuto Imura (Kanazawa University, Japan) and Keita Emura (Kanazawa University, Japan)</i>	
Evading IoT Intrusion Detection Systems with GAN .....	48
<i>Mariama Mbow (Kyushu University, Japan), Rodrigo Roman (Network, Information and Computer Security (NICS) Lab, University of Malaga, Spain), Takeshi Takahashi (National Institute of Information and Communications Technology, Japan), and Kouichi Sakurai (Kyushu University, Japan)</i>	
A Pull Firmware Update Mechanism for Industrial Control Based on IOTA Stream .....	56
<i>Yuon-Chang Lin (National Chung Hsing University, Taiwan) and Ling Bo (Information &amp; Communication Security Laboratory Chunghwa Telecom Laboratories, Taiwan)</i>	
Improving the Performance of IIoT Intrusion Detection System Using Hybrid Synthetic Data .....	62
<i>Chia-Mei Chen (National Sun Yat-sen University, Kaohsiung, Taiwan), Chi-Hsuen Hsu (National Sun Yat-sen University, Kaohsiung, Taiwan), Zheng-Xun Cai (National Sun Yat-sen University, Kaohsiung, Taiwan), Gu-Hsin Lai (Taiwan Police College, Taipei, Taiwan), and Ya-Hui Ou (National Penghu University, Penghu, Taiwan)</i>	
CCADM: A Continuous Collection Scheme for Anonymous Data Management .....	69
<i>Yun-Hsin Chuang (National Cheng Kung University, Taiwan), Po-Wen Chi (National Taiwan Normal University, Taiwan), and Ming-Hung Wang (National Chung Cheng University, Taiwan)</i>	

## Network Security and Application Security

Linear Retention Convolutional Network for Few-Shot Network Threat Detection .....	75
<i>Yong Ding (Guilin University of Electronic Technology, China; Institute of Cyberspace Technology, HKCT Institute for Higher Education, China), Zhi Li (Guilin University of Electronic Technology, China), Changsong Yang (Guilin University of Electronic Technology, China), Hai Liang (Guilin University of Electronic Technology, China), Siyuan Jia (Guilin University of Electronic Technology, China), and Zhenyu Li (Guilin University of Electronic Technology, China)</i>	
Pairing-Free Identity-Based Encryption with Security Against the KGC .....	83
<i>Yi-Fan Tseng (National Chengchi University, Taiwan), Jheng-Jia Huang (National Taiwan University of Science and Technology, Taiwan), Guan-Yu Chen (National Taiwan University of Science and Technology, Taiwan), Wei-Hsueh Wang (National Taiwan University of Science and Technology, Taiwan), and Yu-Hsuan Chang (National Chengchi University, Taiwan)</i>	

An Effective Feature Selection Algorithm for Machine Learning-Based Malicious Traffic Detection .....	91
<i>Chao Fei (Nanjing Normal University, China), Nian Xia (Nanjing Normal University, China), Pang-Wei Tsai (National Cheng Kung University, Taiwan), Yang Lu (Nanjing Normal University, China), Xiaonan Pan (Xi'an Jiaotong-Liverpool University, China), and Junli Gong (Beijing Normal University-Hong Kong Baptist University United International College, China)</i>	
Secure and Portable Anonymous Credentials without Tamper-Resistant Hardware .....	99
<i>Tianshu Yu (Institute of Software Chinese Academy of Sciences University of Chinese Academy of Sciences, China) and Kunpeng Bai (Institute of Software, Chinese Academy of Sciences, China)</i>	
Security Requirements for Fully Automated AI Systems to Exercise and Ensure the Rights of Data Subjects .....	107
<i>Junhyung Park (Soonchunhyang University, Korea), Gunsang You (Soonchunhyang University, Korea), Yeontae Ji (Soonchunhyang University, Korea), and Heung Youl Youm (Soonchunhyang University, Korea)</i>	

## Information Security and Blockchain

Pairing Based Multisignature with Message Flexibility .....	113
<i>Kodai Hayashida (Osaka University, Japan) and Atsuko Miyaji (Osaka University, Japan)</i>	
Backdoored-Input Detection by Trigger Embedding .....	121
<i>Akira Fujimoto (Osaka University, Japan), Shintaro Yamashita (Osaka University, Japan), Yuntao Wang (The University of Electro-Communications, Japan), and Atsuko Miyaji (Osaka University, Japan)</i>	
Proposal for Key-Value Commitments with Offline Batch Update .....	129
<i>Toshiyuki Mineta (Osaka University, Japan), Atsuko Miyaji (Osaka University, Japan), and Hideaki Miyaji (Ritsumeikan University, Japan)</i>	
The Reality and Feature Analysis of Information Diffusion in Japanese Disinformation Examples .....	137
<i>Shuhei Ippa (Institute of Information Security, Japan), Takao Okubo (Institute of Information Security, Japan), and Masaki Hashimoto (Kagawa University, Japan)</i>	
Color Image Steganography with Authentication via Scalable Index Encoding .....	143
<i>Min-Yu Liang (National Chung Hsing University, Taiwan), Yun-Chieh Chang (National Chung Hsing University, Taiwan), and Jason Lin (National Chung Hsing University, Taiwan)</i>	
Adaptive Machine Learning Model For Dynamic Field Selection .....	151
<i>Yu Chi Lin (National Taiwan Normal University, Taiwan) and Po-Wen Chi (National Taiwan Normal University, Taiwan)</i>	

**Author Index** ..... 157