

2024 8th International Conference on Cryptography, Security and Privacy (CSP 2024)

**Osaka, Japan
20-22 April 2024**



**IEEE Catalog Number: CFP24Z50-POD
ISBN: 979-8-3503-8633-2**

**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:	CFP24Z50-POD
ISBN (Print-On-Demand):	979-8-3503-8633-2
ISBN (Online):	979-8-3503-8632-5

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

2024 8th International Conference on Cryptography, Security and Privacy (CSP) **CSP 2024**

Table of Contents

Preface	viii
Organizing Committee	ix
Reviewers	xi

Digital Security and Privacy

An Approach of Privacy-Preserved PQC-Based Cyber-Threat Intelligence System	1
<i>Yu-Jen Chen (Feng Chia University, Taiwan), Tzu-Wei Lin (Feng Chia University, Taiwan), Chung-Wei Kuo (Feng Chia University, Taiwan), and Kuo-Yu Tsai (Feng Chia University, Taiwan)</i>	
WOTS-Based Conditional Privacy-Preserving Authentication Protocol for VANETs	5
<i>Kuo-Yu Tsai (Feng Chia University, Taiwan), Chung-Wei Kuo (Feng Chia University, Taiwan), Li-Chung Leung (Feng Chia University, Taiwan), and Ying-Hsuan Yang (Feng Chia University, Taiwan)</i>	
Linkage Deanonymization Risks, Data-Matching and Privacy: A Case Study	10
<i>William Wong (New York Institute of Technology Vancouver, Canada), Zakaria Alomari (New York Institute of Technology Vancouver, Canada), Yu Liu (York Institute of Technology Vancouver, Canada), and Lloyd Jura (New York Institute of Technology Vancouver, Canada)</i>	
Tuning Pseudonymization Parameters in a Privacy by Design Approach for Secure Information Discovery Between Federated Organizations	17
<i>Ulrich Kriegel (Collaborative Safety and Security ESPRI, Fraunhofer FOKUS, Germany), Sascha Peitzsch (Collaborative Safety and Security ESPRI, Fraunhofer FOKUS, Germany), Hannes Restel (Collaborative Safety and Security ESPRI, Fraunhofer FOKUS, Germany), and Ulrich Meissen (FOKUS HTW Berlin – University of Applied Sciences, Germany)</i>	
A Real-Time Approach to Detecting API Abuses Based on Behavioral Patterns	24
<i>Sameeraa Prinakaa (PES University, India), Bavanika V (PES University, India), Sanjana S (PES University, India), Sneha Srinivasan (PES University, India), and Sarasvathi V (PES University, India)</i>	
An Application Evaluation for Differentially Private Database Release Methods	29
<i>Mathew Nicho (Rabdan Academy, United Arab Emirates), Mrinal Walia (University of Windsor, Canada), and Shafaq Khan (University of Windsor, Canada)</i>	

Digital Encryption and Authentication

A Trust Service Model Adaptable to Various Assurance Levels by Linking Digital IDs and Certificates	38
<i>Junichiro Hayata (Deloitte Tohmatsu Cyber LLC, Japan), Kenta Nomura (Deloitte Tohmatsu Cyber LLC, Japan), Yuta Takata (Deloitte Tohmatsu Cyber LLC, Japan), Hiroshi Kumagai (Deloitte Tohmatsu Cyber LLC, Japan), Masaki Kamizono (Deloitte Tohmatsu Cyber LLC, Japan), Tsuyoshi Kono (Deloitte Tohmatsu Risk Advisory LLC, Japan), Yoshihiro Maeda (Deloitte Touche Tohmatsu LLC, Japan), and Naohisa Fukuda (Japan Communications Inc, Japan)</i>	
A Multi-Receiver Certificateless Signcryption (MCLS) Scheme	46
<i>Alia Umrani (University College Cork, Ireland), Apurova K Vangujar (University College Cork, Ireland), and Paolo Palmieri (University College Cork, Ireland)</i>	
An Analysis of Non-Elliptic Curve Based Primality Tests	53
<i>William Wong (New York Institute of Technology, Canada), Zakaria Alomari (New York Institute of Technology, Canada), Ching Lai (New York Institute of Technology, Canada), Zhida Li (New York Institute of Technology, Canada), and Arif Ullah (Air University, Pakistan)</i>	
PPSC: A Privacy-Preserving Stateless Cryptocurrency System	59
<i>Xingyu Yang (Beijing Institute of Technology, China), Lei Xu (Beijing Institute of Technology, China), and Liehuang Zhu (Beijing Institute of Technology, China)</i>	
Efficient Active and Concurrent-Secure ID-Based Identification from Digital Signature	65
<i>Syh-Yuan Tan (Multimedia University, Malaysia) and Swee-Huay Heng (Multimedia University, Malaysia)</i>	
Arbitration Electronic Contract Scheme Based on Blind Signature	71
<i>Chao Ding (Zhengzhou University, China) and Xiaoyu Li (Zhengzhou University, China)</i>	
Ransomware Defense Empowered: Deep Learning for Real-Time Family Identification with a Proprietary Dataset	77
<i>Hassan Jalil Hadi (Wuhan University, China), Yue Cao (Wuhan University, China), Naveed Ahmad (Prince Sultan University, Riyadh), and Muhammad Ali Alshara (Prince Sultan University, Riyadh)</i>	

Information Security and Image Detection

Research and Analysis of the Effects of Different Shielding Materials on Resisting Side-Channel Attacks on IoT Device Microcontroller	84
<i>Chung-Wei Kuo (Feng-Chia University, Taiwan), Chun-Chang Lin (Feng-Chia University, Taiwan), Yu-Yi Hong (Feng-Chia University, Taiwan), Jia-Ruei Liu (Feng-Chia University, Taiwan), Chun-Hsiu Yeh (Feng-Chia University, Taiwan), and Kuo-Yu Tsai (Feng-Chia University, Taiwan)</i>	
Finding Generators of Ideals in non-Cyclic Number Fields by Using Norm Relations	89
<i>Shixin Tian (University of Chinese Academy of Sciences, Republic of China) and Chang Lv (Institute of Information Engineering, Republic of China)</i>	

An Image Attribute-Based Approach for Generating Minimally Perturbed Images for Face Concealment	94
<i>John Matthew Bainto (De La Salle University, Philippines), Amos Rafael Cacha (De La Salle University, Philippines), John Vincent Chua (De La Salle University, Philippines), Josh Aaron Khyle Uson (De La Salle University, Philippines), Macario II Cordel (Asian Development Bank), Daniel Stanley Tan (Open Universiteit, Netherlands), and Arren Matthew Antioquia (De La Salle University, Philippines)</i>	
A Rapid Fatigue Detection Network for Air Traffic Controller Based on Euler Video Amplification and Attention Mechanism	101
<i>Shanxiu Ma (Nanjing University of Aeronautics and Astronautics, China), Guoqiang Wang (Xinjiang Air Traffic Control Bureau of CAAC, China), Gang Tian (Xinjiang Air Traffic Control Bureau of CAAC, China), and Zhiyuan Shen (Nanjing University of Aeronautics and Astronautics, China)</i>	
Research on Voice Traffic Transmitted Over an IP Network Based on IP PBX Asterisk Under the Use of Various Codecs and Cryptosystems	106
<i>Mubarak Yakubova (Almaty University of Power Engineering and Telecommunications Gumarbek, Kazakhstan), Kuanysh Alipbayev (Almaty University of Power Engineering and Telecommunications Gumarbek, Kazakhstan), and Olga Manankova (International Information Technology University, Kazakhstan)</i>	
Author Index	113