

# **2022 6th International Conference on Cryptography, Security and Privacy (CSP 2022)**

**Tianjin, China  
14-16 January 2022**



**IEEE Catalog Number: CFP22Z50-POD  
ISBN: 978-1-6654-7976-9**

**Copyright © 2022 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:	CFP22Z50-POD
ISBN (Print-On-Demand):	978-1-6654-7976-9
ISBN (Online):	978-1-6654-7975-2

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

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2022 6th International Conference on Cryptography, Security and Privacy (CSP) **CSP 2022**

## Table of Contents

Preface .....	ix
Committee List .....	x
Reviewers .....	xii

### Session 1- Data Encryption and Security

Teleporting Qubits Between Participants by Third-Party Center .....	1
<i>Abdulbast A. Abushgra (Utica College)</i>	
Anonymity-Driven Measures for Privacy .....	6
<i>Sevgi Arca (Texas Tech University, USA) and Rattikorn Hewett (Texas Tech University, USA)</i>	
RippleSign: Isogeny-Based Threshold Ring Signatures with Combinatorial Methods .....	11
<i>Li Li (Peking University, China) and Maozhi Xu (Peking University, China)</i>	
The Processing Goes Far Beyond “the app” – Privacy Issues of Decentralized Digital Contact Tracing using the Example of the German Corona-Warn-App .....	16
<i>Rainer Rehak (Weizenbaum-Institute for the Networked Society, Germany) and Christian R. Kühne (Forum Computer Professionals für Peace and Societal Responsibility (FIF), Germany)</i>	
Evaluation Study on Privacy Policies of Express Companies Based on Cloud Model .....	21
<i>Qian Zhang (Guangdong University of Technology, China), Weihong Xie (Guangdong University of Technology, China), and Xinxian Pan (Guangdong University of Technology, China)</i>	
Differential Privacy under Incalculable Sensitivity .....	27
<i>Tomoaki Mimoto (Advanced Telecommunications Research Institute International (ATR), Japan), Masayuki Hashimoto (Advanced Telecommunications Research Institute International(ATR), Japan), Hiroyuki Yokoyama (Advanced Telecommunications Research Institute International(ATR), Japan), Toru Nakamura (KDDI Research, Inc., Japan), Takamasa Isohara (KDDI Research, Inc., Japan), Ryosuke Kojima (Kyoto University, Japan), Aki Hasegawa (Kyoto University, Japan), and Yasushi Okuno (Kyoto University, Japan)</i>	
Computational Refinements for Post-Quantum Elliptic Curve Security .....	32
<i>Eric Sakk (Morgan State University, USA)</i>	

Analyzing Initial Design Theory Components for Developing Information Security Laboratories .....	36
<i>Sarfraz Iqbal (Linnaeus University, Sweden)</i>	
A Lightweight Advertisement Ecosystem Simulation Platform for Security Analysis .....	41
<i>Chenjia Yu (Harbin Institute of Technology), Mehdi Gheisari (Islamic Azad University, Iran), and Yang Liu (Harbin Institute of Technology)</i>	
A Proactively Defensive Low-Level Decision Center Model of Endogenous Security .....	46
<i>Feilin Li (Southeast University, China), Tao Li (Southeast University, Purple Mountain Laboratories for Network and Communication Security, China), and Aiqu Hu (Southeast University, Purple Mountain Laboratories for Network and Communication Security, China)</i>	

## Session 2- Cyber Attacks and Cybersecurity

Electromagnetic Side-Channel Attack Resilience against PRESENT Lightweight Block Cipher .....	51
<i>Nilupulee A. Gunathilake (Edinburgh Napier University, United Kingdom), Ahmed Al-Dubai (Edinburgh Napier University, United Kingdom), William J. Buchanan (Edinburgh Napier University, United Kingdom), and Owen Lo (Edinburgh Napier University, United Kingdom)</i>	
Context-Based Adblocker using Siamese Neural Network .....	56
<i>Shawn Collins (Old Dominion University, USA), Emily Wu (Princess Anne High School, USA), and Rui Ning (Old Dominion University, USA)</i>	
IoTProtect: A Machine-Learning Based IoT Intrusion Detection System .....	61
<i>Mohammed M. Alani (Seneca College of Applied Arts and Technology, Canada)</i>	
The Future Roadmap for Cyber-Attack Detection .....	66
<i>Raha Soleymanzadeh (Ryerson University, Canada) and Rasha Kashef (Ryerson University, Canada)</i>	
Multifaceted Analysis of Malicious Ethereum Accounts and Corresponding Activities .....	71
<i>Jia Wang (Yokohama National University, Japan), Takayuki Sasaki (Institute of Advanced Sciences, Yokohama National University, Japan), Kazumasa Omote (Faculty of Engineering, Information and Systems, University of Tsukuba, Japan), Katsunari Yoshioka (Yokohama National University, Japan), and Tsutomu Matsumoto (Yokohama National University, Japan)</i>	
Cyber-Security Enhanced Network Meta-Model and its Application .....	80
<i>Xinli Xiong (National University of Defense Technology, China), Liang Guo (National University of Defense Technology, China), Yunfeng Zhang (National University of Defense Technology, China), and Jingye Zhang (National University of Defense Technology, China)</i>	
Cyber Threat Analysis and Trustworthy Artificial Intelligence .....	86
<i>Shuangbao Paul Wang (Morgan State University, USA), Tanvir Arafin (Morgan State University, USA), Onyema Osuagwu (Morgan State University, USA), and Ketchiozo Wandji (Morgan State University, USA)</i>	
CoAP-DoS: An IoT Network Intrusion Data Set .....	91
<i>Jared Mathews (The Citadel, USA), Prosenjit Chatterjee (The Citadel, USA), and Shankar Banik (The Citadel, USA)</i>	

Analysis of the Propagation of Miner Botnet .....	96
<i>Yuxi Cheng (Southeast University, China), Ziang Jin (Southeast University, China), and Wei Ding (Southeast University, China)</i>	
Spectrum-Based Fingerprint Extraction and Identification Method of 100M Ethernet Card .....	102
<i>Jiaqi Liu (Southeast University, China), Aiqun Hu (Southeast University, China), and Sheng Li (Southeast University, China)</i>	

### **Session 3- Computer and Information Security**

A Class of Software-Layer DoS Attacks in Node.js Web Apps .....	108
<i>Tuong Phi Lau (University of Information Technology, Vietnam)</i>	
Vertical Scanning Behavior Analysis of High-Frequency Superpoints .....	114
<i>Wenxian Guo (Southeast University, China), Haiqing Yu (Southeast University, China), and Wei Ding (Southeast University, China)</i>	
The AILA Methodology for Automated and Intelligent Likelihood Assignment .....	119
<i>Giampaolo Bella (Università di Catania, Italy), Cristian Daniele (Radboud University, The Netherlands), and Mario Raciti (INAF –Istituto Nazionale di Astrofisica, Italy)</i>	
From Machine Learning Based Intrusion Detection to Cost Sensitive Intrusion Response .....	124
<i>Tazar Hussain (Ulster University, UK), Alfie Beard (BT Labs, Ipswich UK), Liming Chen (Ulster University, UK), Chris Nugent (Ulster University, UK), Jun Liu (Ulster University, UK), and Adrian Moore (Ulster University, UK)</i>	
Blockchain-Based Identity Discovery between Heterogenous Identity Management Systems .....	131
<i>Marcin Dąbrowski (AGH University of Science and Technology Krakow, Poland) and Piotr Pacyna (AGH University of Science and Technology Krakow, Poland)</i>	
Convex Hull Convolutional Non-negative Matrix Factorization Based Speech Enhancement for Multimedia Communication .....	138
<i>Dongxia Wang (Tianjin University of Technology and Education, Tianjin, China), Jie Cui (Liaoning University of Technology, Jinzhou, China), Jinghua Wang (Tianjin University of Technology and Education, Tianjin, China), Huan Tan (Liaoning University of Technology, Jinzhou, China), and Ming Xu (Liaoning University of Technology, Jinzhou, China)</i>	
An Approach to Construct Feedforward Clock-Controlled Sequence with High Linear Complexity	143
<i>Yangpan Zhang (Peking University, China)</i>	
A Two-Stage Out-Of-Box Method for Detecting Side-Channel Attacks in Cloud Computing .....	148
<i>Jiangyong Shi (National University of Defense, China), Ping Kuang (National University of Defense, China), Yongjun Wang (National University of Defense, China), and Yuexiang Yang (National University of Defense, China)</i>	
Blockchain-Based Smart Parking System using Ring Learning with Errors Based Signature .....	154
<i>Jihan Lailatul Atiqoh (Telkom University, Indonesia), Ari Moesrami Barmawi (Telkom University, Indonesia), and Farah Afianti (Telkom University, Indonesia)</i>	

**Author Index** ..... 159