

# **2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP 2021)**

**Zhuhai, China  
8 – 10 January 2021**



**IEEE Catalog Number: CFP21Z50-POD  
ISBN: 978-1-7281-8622-1**

**Copyright © 2021 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:	CFP21Z50-POD
ISBN (Print-On-Demand):	978-1-7281-8622-1
ISBN (Online):	978-1-7281-8621-4

**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

# Table of Contents

## 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP 2021)

Preface.....	vii
Committees.....	viii

---

### ✧ Cryptographic Theory and Applied Technology

A Scheme of Key Distribution in Smart Grid .....	1
<i>Zhou Youwu, Liu Mingjun, Ye Aimin</i>	
Code Structures for Quantum Encryption and Decryption .....	7
<i>Eric Sakk, Shuangbao Paul Wang</i>	
Unified Attribute-Based Encryption Scheme for Industrial Internet of Things.....	12
<i>Wei Li, Jing Si, Jianhua Xing, Yongjing Zhang, Deli Liu, Zhiyuan Sui</i>	
Quantum Algorithms: Overviews, Foundations, and Speedup .....	17
<i>Shuangbao Paul Wang, Eric Sakk</i>	
Assessment of Remote Biometric Authentication Systems: Another Take on the Quest to Replace Passwords .....	22
<i>Daniel Köhler, Eric Klieme, Matthias Kreuzeler, Feng Cheng, Christoph Meinel</i>	
Automatic Test Case Generation for Vulnerability Analysis of Galois Field Arithmetic Circuits.....	32
<i>Krishn Kumar Gupt, Meghana Kshirsagar, Joseph P. Sullivan, Conor Ryan</i>	

### ✧ Data Security and Blockchain Technology

Investigating the Compliance of the GDPR: Processing Personal Data On A Blockchain.....	38
<i>Michelle Poelman, Sarfraz Iqbal</i>	
Analysis and Improvements to the Special Number Field Sieve for Discrete Logarithm Problems.....	45
<i>Liwei Liu, Maozhi Xu, Guoqing Zhou</i>	
Trust Evaluation Algorithm based on Association Rule Extraction .....	50
<i>Yanchun Cui, Kai Zhong, Ansheng Yin</i>	

DOSing Distributed Ledger Technology: IOTA.....	55
<i>Mark A. Brady, Ikram Ullah, Paul J. M. Havinga</i>	
<i>velink</i> - A Blockchain-based Shared Mobility Platform for Private and Commercial Vehicles utilizing ERC-721 Tokens .....	62
<i>Dominic Pirker, Thomas Fischer, Harald Witschnigy, Christian Steger</i>	
Lightweight Blockchain-based Platform for GDPR-Compliant Personal Data Management .....	68
<i>Cristófol Daudén-Esmel, Jordi Castellà-Roca, Alexandre Viejo and Josep Domingo-Ferrer</i>	
✧ Privacy Protection and Safety Inspection	
A Blockchain-based Privacy-Preserving Recommendation Mechanism .....	74
<i>Liangjie Lin, Yuchen Tian, Yang Liu</i>	
A Novel Edge Computing Offloading and Privacy-preserving Scheme for Energy Internet.....	79
<i>Kunchang Li, Xu Han, Yifan Yang, Shuhao Wang, Runhua Shi, Jianbin Li</i>	
ECDSA-Compatible Privacy Preserving Signature with Designated Verifier .....	84
<i>Sam Ng, Tomas Tauber, Leslie Cheung</i>	
PRADroid: Privacy Risk Assessment for Android Applications.....	90
<i>Yang Yang, Xuehui Du, Zhi Yang</i>	
A Study on Privacy Issues in Internet of Things (IoT) .....	96
<i>Naqliyah Zainuddin, Maslina Daud, Sabariah Ahmad, Mayasarah Maslizan, Syafiq Anneisa Leng Abdullah</i>	
Dimensionality-reduced Secure Outlier Detection on Union of Subspaces .....	101
<i>Kunzan Liu, Yuchen Jiao, Ye Jin, Xu Xiang, Yuantao Gu</i>	
SpaML: a Bimodal Ensemble Learning Spam Detector based on NLP Techniques.....	107
<i>Jaouhar Fattahi, Mohamed Mejri</i>	
A LSTM-Based Channel Fingerprinting Method for Intrusion Detection.....	113
<i>Ting Ma, Feng Hu, Maode Ma</i>	
DECH: A Novel Attack Pattern of Cloud Environment and Its Countermeasures .....	117
<i>Haoyu Gao, Leixiao Li, Hao Lin, Jianxiong Wan, Dan Deng, Jie Li</i>	
✧ Software and information Security	
A Partial-Lifting-Based Compiling Concolic Execution Approach .....	123
<i>Haotian Zhang, Weiyu Dong, Jian Lin</i>	

Detecting Android Malware Based on Dynamic Feature Sequence and Attention Mechanism.....	129
<i>Hanlin Long, Zhicheng Tian, Yang Liu</i>	
The Influence of Mobile Operating Systems on User Security Behavior.....	134
<i>Martin Butler, Rika Butler</i>	
DGA Domain Detection using Deep Learning.....	139
<i>Haleh Shahzad, Abdul Rahman Sattar, Janahan Skandaraniyam</i>	
Research on Malware Variant Detection Method Based on Deep Neural Network .....	144
<i>Xing Jianhua, Si Jing, Zhang Yongjing, Li Wei, Zheng Yuning</i>	
Mobile Firewall applications: an analysis of usability and effectiveness .....	148
<i>Wouter Louman, Mitchell Vernee, Danique de Bruijn, Babette van 't Riet, Hani Alers</i>	
✧ Communication and Network Security	
Trend Analysis and Countermeasure Research of DDoS Attack under 5G Network.....	153
<i>Haiou Huang, Jianfeng Chu, Xiaochun Cheng</i>	
Multi-user broadcast authenticaiton in Power LTE Private Network with Compressed Bloom Filter .....	161
<i>Gaofeng Zhao, Rui Liu, Yang Li, Jin Huang, Mingxuan Zhang, Weiwei Miao</i>	
Power IoT security protection architecture based on zero trust framework .....	166
<i>Zhang Xiaojian, Chen Liandong, Fan Jie, Wang Xiangqun, Wang Qi</i>	
Outage Performance of Satellite-UAV Network Framework based on NOMA.....	171
<i>Changqing Wang, Xiangyu Yang, Quancheng Du, Jiexiang Wang</i>	
SARG04 and AK15 Protocols Based on the Run-Time Execution and QBER.....	176
<i>Abdulbast A. Abushgra</i>	
✧ Image Processing and Information Security	
Using Boltzmann Entropy to Measure Scrambling Degree of Grayscale Images.....	181
<i>Xinghua Cheng and Zhilin Li</i>	
ZeroDVS: Trace-Ability and Security Detection of Container Image Based on Inheritance Graph .....	186
<i>Yan Zheng, Weiyu Dong, Jiangtao Zhao</i>	
Damaged Fingerprint Recognition by Convolutional Long Short-Term Memory Networks for Forensic Purposes .....	193
<i>Jaouhar Fattahi and Mohamed Mejri</i>	

Forensic Analysis of Binary Structures of Video Files .....	200
<i>Md Abir Hasan, Orion Lawlor, Nusrat Jahan</i>	
License Plate Detection Using Bayesian Method Based on Edge Features.....	205
<i>Xinyun Yan, Chishe Wang, Dahui Hao, Min Chen</i>	
Author Index	