

2023 7th International Conference on Cryptography, Security and Privacy (CSP 2023)

**Tianjin, China
21-23 April 2023**



**IEEE Catalog Number: CFP23Z50-POD
ISBN: 979-8-3503-2337-5**

**Copyright © 2023 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:	CFP23Z50-POD
ISBN (Print-On-Demand):	979-8-3503-2337-5
ISBN (Online):	979-8-3503-2336-8

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

2023 7th International Conference on Cryptography, Security and Privacy (CSP) **CSP 2023**

Table of Contents

Preface	viii
Program Committee	ix
Reviewers	xi

Data Network and Network Security

Two Dimensional SOST: Extract Multi-Dimensional Leakage for Side-Channel Analysis on Cryptosystems	1
<i>Zheng Liu (Beijing Institute of Technology; State Key Laboratory of Cryptology, China), Congming Wei (Beijing Institute of Technology; Hanzhou Normal University, China), Shengjun Wen (State Administration for Market Regulation, China), Shaofei Sun (Beijing Institute of Technology, China), Yaoling Ding (Beijing Institute of Technology; Institute of Information Engineering, Chinese Academy of Sciences), China), and An Wang (Beijing Institute of Technology; State Key Laboratory of Cryptology, China)</i>	
Classification and Application of Long-Duration Flows Based on Flow Behavior	7
<i>Zihao Chen (Southeast University, China), Wei Ding (Southeast University, China), Weijian Sun (Southeast University, China), and Liang Xu (Southeast University, China)</i>	
Protecting UAV-Networks: A Secure Lightweight Authentication and Key Agreement Scheme	13
<i>Hulya Dogan (Swansea University, United Kingdom)</i>	
A Related Key Attack on the Word-Oriented BeepBeep Stream Cipher	22
<i>Zhiyi Liao (PLA SSF Information Engineering University, China), Lin Ding (PLA SSF Information Engineering University, China), and Zheng Wu (PLA SSF Information Engineering University, China)</i>	
Authenticated Identity-Based Encryption Scheme with Equality Test for Cloud-Based Social Network	27
<i>Jiaojiao Du (South China Agricultural University, China), Sha Ma (South China Agricultural University, China), Tian Yang (South China Agricultural University, China), and Qiong Huang (South China Agricultural University, China)</i>	
Cryptomining Traffic Detection Based on BiGRU and Attention Mechanism	35
<i>Yijie Huang (Southeast University, China), Wei Ding (Southeast University, China), and Yuxi Cheng (Southeast University, China)</i>	

Software and Information Security

Post-Mortem of Mega Hacks - Signifying the Need for a Systemic Enterprise View on Information Security	41
<i>Lars Magnusson (Linnaeus University, Sweden) and Sarfraz Iqbal (Linnaeus University, Sweden)</i>	
Detection of Conflicts Between APP's Privacy Policy and Actual Behavior: A Security Analysis System	47
<i>Tong Wu (Harbin Institute of Technology;Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies, China), Qinbo Liu (Harbin Institute of Technology, China), Binchang Li (Harbin Institute of Technology, China), Feng Luo (Harbin Institute of Technology, China), Weilong Li (Harbin Institute of Technology, China), and Yang Liu (Harbin Institute of Technology, China)</i>	
Mission-Oriented Security Framework: An Approach to Embrace Cyber Resilience in Design and Action	54
<i>Xinli Xiong (National University of Defense Technology;Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, China), Qian Yao (National University of Defense Technology;Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, China), and Qiankun Ren (National University of Defense Technology;Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, China)</i>	
A Survey on Cross-Chain Data Transfer	59
<i>Wei Zheng (Hainan University;Oxford-Hainan Blockchain Research Institute, China), Ning Tian (Hainan University, China;The University of Warwick, UK), Kejie Zhao (Hainan University, China), Hong Lei (Hainan University;SSC Holding Company Ltd., China), and Zhiwei Liu (Hainan University;Oxford-Hainan Blockchain Research Institute, China)</i>	
A Multi-Strategy Adversarial Attack Method for Deep Learning Based Malware Detectors	66
<i>Wang Yang (Southeast University, China) and Fan Yin (Southeast University, China)</i>	
A Case Study of Internet Banking Security of Banks Operated in Bangladesh	71
<i>S. M. Mizanur Rahman (Bangladesh University of Professionals, Bangladesh) and Md. Golam Rabiul Alam (Brac University, Bangladesh)</i>	
White-Box PRNG: A Secure Pseudo-Random Number Generator Under the White-Box Attack Model .	77
<i>Weijie Deng (South China Normal University, China)</i>	

Information Privacy Protection and Data Security

A Personal Privacy Risk Assessment Framework Based on Disclosed PII	86
<i>Ningning Wu (University of Arkansas at Little Rock, USA) and Robinson Tamilselvan (University of Arkansas at Little Rock, USA)</i>	
NIC Fingerprint-Based Switch Access Control Technology	92
<i>Kaiwen Sheng (Southeast University, China), Aiqun Hu (Southeast University, China), and Sheng Li (Southeast University, China)</i>	

Secure Multiparty Computation with Identifiable Abort and Fairness	99
<i>Long Nie (Yunnan University, China), ShaoWen Yao (Yunnan University, China), and Jing Liu (Yunnan University, China)</i>	
Generating -Closed Partitions of Datasets with Multiple Sensitive Attributes	107
<i>Vikas Thammanna Gowda (Wichita State University, USA) and Rajiv Bagai (Wichita State University, USA)</i>	
Design and Implementation of a Data Stream Anonymization Core on FPGA	112
<i>Bilal Moussa (University of Technology Belfort-Montbeliard, France;Houmal Technology Park, Lebanon), Kabalan Chaccour (Antonine University, Lebanon;University of Technology Belfort-Montbeliard, France), Mohamad Mroue (Houmal Technology Park, Lebanon;Lebanese University, Lebanon), and Rachid Bouyekhf (University of Technology Belfort-Montbeliard, France)</i>	
Efficient Privacy-Preserving Data Aggregation for Lightweight Secure Model Training in Federated Learning	119
<i>Cong Hu (State Grid Anhui Electric Power Information & Telecommunication Co., Ltd., China), Shuang Wang (Anhui Mingsheng Hengzhuo Technology Co., Ltd., China), Cuiling Liu (State Grid Anhui Electric Power Information & Telecommunication Co., Ltd., China), and Tingzeng Zhang (Anhui Mingsheng Hengzhuo Technology Co., Ltd., China)</i>	
Inference Rules for Determined Decisions in Policy-Based ABAC Enforcement Systems	124
<i>Bach-Hue Pham (University of Science, Viet Nam National University, VietNam), Toan-Thinh Truong (University of Science, Viet Nam National University, VietNam), and Minh-Triet Tran (University of Science, Viet Nam National University Ho Chi Minh City, VietNam)</i>	
An Application Service for Supporting Security Management In Software-Defined Networks	129
<i>Mohamed Ousama Ben Miloud (University of North Dakota, USA) and Jun Liu (University of North Dakota, USA)</i>	

Modern Password Theory and Information Encryption Technology

Verifiable Threshold Multiplication Protocol Based on Oblivious Transfer	134
<i>Sam Ng (Crypto.com, Hong Kong), Tomas Tauber (Crypto.com, Hong Kong), and Leslie Cheung (Crypto.com, Hong Kong)</i>	
An Improved Key Mismatch Attack on Kyber	140
<i>Yaru Wang (State Key Laboratory of Mathematical Engineering and Advanced Computing, China), Haodong Jiang (State Key Laboratory of Mathematical Engineering and Advanced Computing, China), and Zhi Ma (State Key Laboratory of Mathematical Engineering and Advanced Computing, China)</i>	
Secure Search over Multi-key Homomorphically Encrypted Data	145
<i>Buvana Ganesh (University College Cork, Ireland) and Paolo Palmieri (University College Cork, Ireland)</i>	
Computation on Jacobians of Hyperelliptic Curves of Genus 3	152
<i>Zhili Dong (University of Chinese Academy of Science, China), Minzhong Luo (University of Chinese Academy of Science, China), and Chang Lv (Institute of Information Engineering, CAS, China)</i>	

Quantum Key Distribution and Security Studies	158
<i>Jianzhou Mao (Morgan State Univeristy, USA), Guobin Xu (Morgan State University, USA), Eric Sakk (Morgan State University, USA), and Shuangbao Paul Wang (Morgan State University, USA)</i>	
An Efficient Public Key Encryption With Set Equality Test	163
<i>Xu Zhang (South China Agricultural University, China), Sha Ma (South China Agricultural University, China), Chengyu Jiang (South China Agricultural University, China), and Pan Zhou (South China Agricultural University, China)</i>	
An Improved DEFAULT-Like Cipher via Dynamic Secret S-Boxes Against Differential Fault Attack	170
<i>Linyang Yan (Guilin University Of Electronic Technology, China), Huijiao Wang (Guilin University Of Electronic Technology, China), and Yongzhuang Wei (Guilin University Of Electronic Technology, China)</i>	
Hill Cipher Modifications and Dynamic Cryptosystem Design	176
<i>MengZe Hong (University of Nottingham Malaysia, Malaysia) and Wing Loon Chee (University of Nottingham Malaysia, Malaysia)</i>	
A New Research on Verifiable and Searchable Encryption Scheme Based on Blockchain	181
<i>Zhong Kang (Central University of Finance and Economics, China) and Maoning Wang (Central University of Finance and Economics, China)</i>	
AES128 Encrypted Image Classification	186
<i>Aidana Irmanova (Nazarbayev University, Kazakhstan) and Martin Lukac (Nazarbayev University, Kazakhstan)</i>	
haydIT : An Encryptor and Decryptor Application	191
<i>Marlon A. Diloy (National University, Philippines), Joan Katherine N. Romasanta (National University, Philippines), Marco Paulo J. Burgos (National University, Philippines), Carlito O. Loyola Jr. (National University, Philippines), Leandro R. De Luna (National University, Philippines), and Geanne Ross L. Franco (De La Salle University, Philippines)</i>	
Author Index	197