

# **2020 15th Asia Joint Conference on Information Security (AsiaJCIS 2020)**

**Taipei, Taiwan  
20-21 August 2020**



**IEEE Catalog Number: CFP2033T-POD  
ISBN: 978-1-7281-9923-8**

**Copyright © 2020 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:	CFP2033T-POD
ISBN (Print-On-Demand):	978-1-7281-9923-8
ISBN (Online):	978-1-7281-9922-1

**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

# 2020 15th Asia Joint Conference on Information Security (AsiaJCIS) **AsiaJCIS 2020**

## Table of Contents

Message from the General Co-Chairs	ix
Message from the Program Co-Chairs	x
Conference Organization	xi
Program Committee	xiii
Steering Committee	xv
Reviewers	xvi
Sponsors	xvii
Supporters	xviii

### Session 1: Cryptosystem I

A Generic Construction of Predicate Proxy Key Re-Encapsulation Mechanism	1
<i>Yi-Fan Tseng (National Chengchi University), Zi-Yuan Liu (National Chengchi University), and Raylin Tso (National Chengchi University)</i>	
Key-Aggregate Proxy Re-Encryption with Dynamic Condition Generation Using Multilinear Map	9
<i>Chun-I Fan (National Sun Yat-sen University), Yi-Fan Tseng (National Chengchi University), and Yen-Lin Huang (National Sun Yat-sen University)</i>	
Practical Query-Based Order Revealing Encryption from Symmetric Searchable Encryption	16
<i>Masayuki Yoshino (Hitachi, Ltd.), Ken Naganuma (Hitachi, Ltd., The University of Tokyo), Noboru Kunihiro (University of Tsukuba), and Hisayoshi Sato (Hitachi, Ltd.)</i>	

### Session 2: Cryptosystem II

Linear Lossy Identification Scheme Derives Tightly-Secure Multisignature	24
<i>Masayuki Fukumitsu (Hokkaido Information University) and Shingo Hasegawa (Tohoku University)</i>	
Post-Quantum zk-SNARK for Arithmetic Circuits using QAPs	32
<i>Ken Naganuma (Hitachi, Ltd. The University of Tokyo), Masayuki Yoshino (Hitachi, Ltd.), Atsuo Inoue (Hitachi Solutions, Ltd.), Yukinori Matsuoka (Hitachi Solutions, Ltd.), Mineaki Okazaki (Hitachi Solutions Create, Ltd.), and Noboru Kunihiro (University of Tsukuba)</i>	

Secure and Flexible Algorithm for Outsourcing of Bilinear Pairings Effectively Resisting Conspiracy .40.....	
	<i>Chih-Hung Wang (National Chiayi University) and Guo-Cyuan Mao (National Chiayi University)</i>

### Session 3: Key Exchange, Distribution, and Management

SIT: Supersingular Isogeny Tree-Based Group Key Exchange .46.....	
	<i>Hector B. Hougaard (Osaka University) and Atsuko Miyaji (Osaka University)</i>
New Secret Key Management Technology for Blockchains from Biometrics Fuzzy Signature .54.....	
	<i>Ken Naganuma (Hitachi, Ltd. The University of Tokyo), Takayuki Suzuki (Hitachi, Ltd.), Masayuki Yoshino (Hitachi, Ltd.), Kenta Takahashi (Hitachi, Ltd.), Yosuke Kaga (Hitachi, Ltd.), and Noboru Kunihiro (University of Tsukuba)</i>
A Time Bound Dynamic Group Key Distribution Scheme with Anonymous Three-Factor Identification for IoT-Based Multi-Server Environments .59.....	
	<i>Chien-Lung Hsu (Chang Gung University) and Tuan-Vinh Le (Chang Gung University)</i>
Cryptanalysis of Four Biometric Based Authentication Schemes with Privacy-Preserving for Multi-Server Environment and Design Guidelines .66.....	
	<i>Yun-Hsin Chuang (National Taiwan University), Chin-Laung Lei (National Taiwan University), and Hung-Jr Shiu (Tunghai University)</i>

### Session 4: Privacy and Anonymity

Hierarchical One-out-of-Many Proofs With Applications to Blockchain Privacy and Ring Signatures .74.....	
	<i>Aram Jivanyan (Zcoin) and Tigran Mamikonyan (Zcoin)</i>
Multi-Value Private Information Retrieval using Homomorphic Encryption .82.....	
	<i>Hsiang-Chen Hsu (National Chengchi University), Zi-Yuan Liu (National Chengchi University), Raylin Tso (National Chengchi University), and Kung Chen (National Chengchi University)</i>
Privacy Preserving Data Integration Protocol .89.....	
	<i>Atsuko Miyaji (Osaka University) and Yoshitaka Nagao (Osaka University)</i>
An Enhanced Mondrian Anonymization Model Based on Self-Organizing Map .97.....	
	<i>Peter Shaojui Wang (Chunghwa Telecom Laboratories), Pin-Yen Huang (National Chengchi University), Yu-An Tsai (National Chengchi University), and Raylin Tso (National Chengchi University)</i>

## Session 5: Authentication and Verification

- Effective Classification for Multi-Modal Behavioral Authentication on Large-Scale Data .101.....  
*Shuji Yamaguchi (Yahoo Japan Corporation), Hidehito Gomi (Yahoo Japan Corporation), Ryosuke Kobayashi (The University of Tokyo), Tran Phuong Thao (The University of Tokyo), Mhd Irvan (The University of Tokyo), and Rie Shigetomi Yamaguchi (The University of Tokyo)*
- 3D-Playfair Encrypted Message Verification Technology Based on MD5 .110.....  
*Wen-Chung Kuo (National Yunlin University of Science & Technology), Wan-Hsuan Kao (National Yunlin University of Science & Technology), Chun-Cheng Wang (National Yunlin University of Science & Technology), and Yu-Chih Huang (Tainan University of Technology)*
- The Empirical Study of Passwords Analysis in Access Point with Specific-Rules and Graphic Process Units .115.....  
*Chia-Mei Chen (National Dr. Sun Yat-sen University), Tien-Ho Chang (National Dr. Sun Yat-sen University), and Gu-Hsin Lai (Taiwan Police College)*
- An Efficient Blockchain-Based Firmware Update Framework for IoT Environment .121.....  
*Meng-Hsuan Tsai (National Taiwan University of Science and Technology), Yu-Cheng Hsu (National Taiwan University of Science and Technology), and Nai-Wei Lo (National Taiwan University of Science and Technology)*

## Session 6: Detection

- A Privacy-Preserving Federated Learning System for Android Malware Detection Based on Edge Computing .128.....  
*Ruei-Hau Hsu (National Sun Yat-sen University), Yi-Cheng Wang (National Sun Yat-sen University), Chun-I Fan (National Sun Yat-sen University), Bo Sun (National Institute of Information and Communications Technology), Tao Ban (National Institute of Information and Communications Technology), Takeshi Takahashi (National Institute of Information and Communications Technology), Ting-Wei Wu (National Sun Yat-sen University), and Shang-Wei Kao (National Sun Yat-sen University)*
- Analysis of Malicious Email Detection using Cialdini's Principles .137.....  
*Hiroki Nishikawa (Mitsubishi Electric Corporation and Shizuoka University), Takumi Yamamoto (Mitsubishi Electric Corporation), Bret Harsham (Mitsubishi Electric Research Laboratories), Ye Wang (Mitsubishi Electric Research Laboratories), Kota Uehara (Shizuoka University), Chiori Hori (Mitsubishi Electric Research Laboratories), Aiko Iwasaki (Mitsubishi Electric Corporation), Kiyoto Kawachi (Mitsubishi Electric Corporation), and Masakatsu Nishigaki (Shizuoka University)*

IoT-Malware Detection Based on Byte Sequences of Executable Files .143.....  
*Tzu-Ling Wan (National Taiwan University of Science and Technology),  
Tao Ban (National Institute of Information and Communications  
Technology), Yen-Ting Lee (National Taiwan University of Science and  
Technology), Shin-Ming Cheng (National Taiwan University of Science  
and Technology), Ryoichi Isawa (National Institute of Information and  
Communications Technology), Takeshi Takahashi (National Institute of  
Information and Communications Technology), and Daisuke Inoue  
(National Institute of Information and Communications Technology)*

Anomaly Detection using Clustered Deep One-Class Classification .151.....  
*Younghwan Kim (Korea University) and Huy Kang Kim (Korea University)*

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