

2019 IEEE Conference on Dependable and Secure Computing (DSC 2019)

**Hangzhou, China
18 – 20 November 2019**



**IEEE Catalog Number: CFP19J65-POD
ISBN: 978-1-7281-2320-2**

**Copyright © 2019 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:	CFP19J65-POD
ISBN (Print-On-Demand):	978-1-7281-2320-2
ISBN (Online):	978-1-7281-2319-6

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

Table of Contents

Securing Relational Database Storage with Attribute Association Aware Shuffling	1
<i>Tieming Geng, Hatim Alsuwat, Chin-Tser Huang, and Csilla Farkas</i>	
Towards a Ledger-Assisted Architecture for Secure Query Processing over Distributed IoT Data	9
<i>Xingliang Yuan, Chengjun Cai, Qian Wang, and Qi Li</i>	
Examining the Robustness of Learning-Based DDoS Detection in Software Defined Networks.....	17
<i>Ahmed Abusnaina, Aminollah Khormali, DaeHun Nyang, Murat Yuksel, and Aziz Mohaisen</i>	
Lightweight Attribute-Based Keyword Search with Policy Protection for Cloud-Assisted IoT	25
<i>Jianfei Sun, Hu Xiong, Robert H. Deng, Yinghui Zhang, Ximeng Liu, and Mingsheng Cao</i>	
MicroGuard: Securing Bare-Metal Microcontrollers against Code-Reuse Attacks	33
<i>Majid Salehi, Danny Hughes, and Bruno Crispo</i>	
Honor among Thieves: Towards Understanding the Dynamics and Interdependencies in IoT Botnets	41
<i>Jinchun Choi, Ahmed Abusnaina, Afsah Anwar, An Wang, Songqing Chen, DaeHun Nyang, and Aziz Mohaisen</i>	
Secure Boolean Queries over Encrypted Data from Indistinguishability Obfuscation	49
<i>Jing Yao, Helei Cui, and Xiaolin Gui</i>	
BanFEL: A Blockchain Based Smart Contract for Fair and Efficient Lottery Scheme	57
<i>Jiasheng Li, Zijian Zhang, and Meng Li</i>	
Fidelity: Towards Measuring the Trustworthiness of Neural Network Classification	65
<i>Ziqi Yang</i>	
DT-Track: Using DNS-Timing Side Channel for Mobile User Tracking.....	73
<i>Chun-Han Lin, Shan-Hsin Lee, Hsiu-Chuan Huang, Chi-Wei Wang, Chia-Wei Hsu, and ShihPyng Shieh</i>	
Traceable Private Set Intersection in Cloud Computing	81
<i>Tao Jiang and Xu Yuan</i>	
Persistent Fault Injection in FPGA via BRAM Modification.....	88
<i>Yiran Zhang, Fan Zhang, Bolin Yang, Guorui Xu, Bin Shao, Xinjie Zhao, and Kui Ren</i>	
A Blind Signature from Module Lattices	94
<i>Huy Quoc Le, Willy Susilo, Thanh Xuan Khuc, Minh Kim Bui, and Dung Hoang Duong</i>	
Random Delay Attack and Its Applications on Load Frequency Control of Power Systems	102
<i>Yongdong Wu, Jian Weng, Bo Qiu, Zhuo Wei, Fan Qian, and Robert H. Deng</i>	
Towards the Trust-Enhancements of Single Sign-On Services	110
<i>Xuhua Bao, Xiaokun Zhang, Jingqiang Lin, Dawei Chu, Qiong Xiao Wang, and Fengjun Li</i>	
E2E Verifiable Electronic Voting System for Shareholders.....	118
<i>Samiran Bag and Feng Hao</i>	
Randomized Positioning DSSS with Message Shuffling for Anti-Jamming Wireless Communications	126
<i>Ahmad Alagil and Yao Liu</i>	

Secure Outsourcing Algorithm for Bilinear Pairings without Pre-Computation	134
<i>Le Tong, Jia Yu, and Hanlin Zhang</i>	
Correlation-Based Search against Friendly Jamming Data Exchange Schemes.....	141
<i>Jingyi Zhang, Qiao Hu, and Gerhard Petrus Hancke</i>	
Super Payment Channel for Decentralized Cryptocurrencies.....	149
<i>Shengmin Xu, Jiaming Yuan, Yingjiu Li, Ximeng Liu, and Yinghui Zhang</i>	
Defeating Speculative-Execution Attacks on SGX with HYPERRACE	157
<i>Guoxing Chen, Mengyuan Li, Fengwei Zhang, and Yinqian Zhang</i>	
SoK: A Systematic Study of Anonymity in Cryptocurrencies	165
<i>Nasser Alsalami and Bingsheng Zhang</i>	
Securely Perturb Big Data by using Inner Product	174
<i>Mingli Wu and Tsz Hon Yuen</i>	
An Optimized Positive-Unlabeled Learning Method for Detecting a Large Scale of Malware Variants	182
<i>Jixin Zhang, Mohammad Faham Khan, Xiaodong Lin, and Zheng Qin</i>	
Gaussian Process Learning for Distributed Sensor Networks under False Data Injection Attacks	190
<i>Xiuming Liu and Edith Ngai</i>	
Utilizing Public Blockchains for Censorship-Circumvention and IoT Communication	196
<i>Nasser Alsalami and Bingsheng Zhang</i>	
Neural Cryptanalysis: Metrics, Methodology, and Applications in CPS Ciphers	203
<i>Ya Xiao, Qingying Hao, and Danfeng (Daphne) Yao</i>	
Proof of Encryption: Enforcement of Security Service Level Agreement for Encryption Outsourcing.....	211
<i>Sultan Alasmari, Weichao Wang, Tuanfa Qin, and Yu Wang</i>	
Multi-Level Proactive Security Auditing for Clouds	219
<i>Suryadipta Majumdar, Azadeh Tabiban, Meisam Mohammady, Alaa Oqaily, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi</i>	
Federated-Cloud Based Deep Neural Networks with Privacy Preserving Image Filtering Techniques	227
<i>Isabelle Choi, Qiyang Song, and Kun Sun</i>	
Exploiting Mallows Distance to Quantify EEG Distribution for Personal Identification.....	235
<i>Baicheng Chen, Kun Woo Cho, Chenhan Xu, Feng Lin, Zhanpeng Jin, and Wen Yao Xu</i>	
Deep-BIF: Blind Image Forensics Based on Deep Learning	243
<i>Baole Wei, Min Yu, Kai Chen, and Jianguo Jiang</i>	
Broken Relationship of Mobile User Intentions and Permission Control of Shared System Resources (Invited Paper).....	249
<i>Hao Wu, Zheng Qin, Xuejin Tian, Edward Sun, Fengyuan Xu, and Sheng Zhong</i>	