

Contents

Crypto Algorithms and Applications

Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems	3
<i>Michal Kedziora, Yang-Wai Chow, and Willy Susilo</i>	
Security Analysis of a Design Variant of Randomized Hashing.	14
<i>Praveen Gauravaram, Shoichi Hirose, and Douglas Stebila</i>	
Secure Two-Party Computation Using an Efficient Garbled Circuit by Reducing Data Transfer.	23
<i>Mohammad Hossein Yalame, Mohammad Hossein Farzam, and Siavash Bayat-Sarmadi</i>	
An Efficient Non-transferable Proxy Re-encryption Scheme	35
<i>S. Sharmila Deva Selvi, Arinjita Paul, and C. Pandu Rangan</i>	
Rounding Technique’s Application in Schnorr Signature Algorithm: Known Partially Most Significant Bits of Nonce.	48
<i>Wenjie Qin and Kewei Lv</i>	
On the Practical Implementation of Impossible Differential Cryptanalysis on Reduced-Round AES	58
<i>Sourya Kakarla, Srinath Mandava, Dhiman Saha, and Dipanwita Roy Chowdhury</i>	

Privacy Preserving Techniques

Private Distributed Three-Party Learning of Gaussian Mixture Models.	75
<i>Kaleb L. Leemaqz, Sharon X. Lee, and Geoffrey J. McLachlan</i>	
A Privacy Preserving Platform for MapReduce	88
<i>Sibghat Ullah Bazai, Julian Jang-Jaccard, and Xuyun Zhang</i>	
Privacy-Preserving Deep Learning: Revisited and Enhanced.	100
<i>Le Trieu Phong, Yoshinori Aono, Takuya Hayashi, Lihua Wang, and Shiho Moriai</i>	

Attacks

Characterizing Promotional Attacks in Mobile App Store.	113
<i>Bo Sun, Xiapu Luo, Mitsuaki Akiyama, Takuya Watanabe, and Tatsuya Mori</i>	

Low-Data Complexity Attacks on Camellia 128
Takeru Koie, Takanori Isobe, Yosuke Todo, and Masakatu Morii

RESTful Is Not Secure 141
Tetiana Yarygina

Malware and Malicious Events Detection

UnitecDEAMP: Flow Feature Profiling for Malicious Events Identification
in Darknet Space. 157
Ruibin Zhang, Chi Yang, Shaoning Pang, and Hossein Sarrafzadeh

A Hybrid Approach for Malware Family Classification 169
*Naqqash Aman, Yasir Saleem, Fahim H. Abbasi,
and Farrukh Shahzad*

Low-Complexity Signature-Based Malware Detection for IoT Devices. 181
Muhammed Fauzi Bin Abbas and Thambipillai Srikanthan

System and Network Security

De-anonymous and Anonymous Technologies
for Network Traffic Release 193
Xiang Tian, Yu Wang, Yujia Zhu, Yong Sun, and Qingyun Liu

Privacy-Aware Authentication for Wi-Fi Based Indoor
Positioning Systems. 201
Sang Guun Yoo and Jhonattan J. Barriga

On the Effectiveness of Non-readable Executable Memory Against BROP. 214
Christian Otterstad

Author Index 223



<http://www.springer.com/978-981-10-5420-4>

Applications and Techniques in Information Security
8th International Conference, ATIS 2017, Auckland, New
Zealand, July 6–7, 2017, Proceedings
Batten, L.; Kim, D.S.; Zhang, X.; Li, G. (Eds.)
2017, XIV, 223 p. 68 illus., Softcover
ISBN: 978-981-10-5420-4