## Contents

### Crypto Algorithms and Applications

- Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems
  
  *Michal Kedziora, Yang-Wai Chow, and Willy Susilo*  
  Page 3

- Security Analysis of a Design Variant of Randomized Hashing
  
  *Praveen Gauravaram, Shoichi Hirose, and Douglas Stebila*  
  Page 14

- Secure Two-Party Computation Using an Efficient Garbled Circuit by Reducing Data Transfer
  
  *Mohammad Hossein Yalame, Mohammad Hossein Farzam, and Siavash Bayat-Sarmadi*  
  Page 23

- An Efficient Non-transferable Proxy Re-encryption Scheme
  
  *S. Sharmila Deva Selvi, Arinjita Paul, and C. Pandu Rangan*  
  Page 35

- Rounding Technique’s Application in Schnorr Signature Algorithm: Known Partially Most Significant Bits of Nonce
  
  *Wenjie Qin and Kewei Lv*  
  Page 48

- On the Practical Implementation of Impossible Differential Cryptanalysis on Reduced-Round AES
  
  *Sourya Kakarla, Srinath Mandava, Dhiman Saha, and Dipanwita Roy Chowdhury*  
  Page 58

### Privacy Preserving Techniques

- Private Distributed Three-Party Learning of Gaussian Mixture Models
  
  *Kaleb L. Leemaqz, Sharon X. Lee, and Geoffrey J. McLachlan*  
  Page 75

- A Privacy Preserving Platform for MapReduce
  
  *Sibghat Ullah Bazai, Julian Jang-Jaccard, and Xuyun Zhang*  
  Page 88

- Privacy-Preserving Deep Learning: Revisited and Enhanced
  
  *Le Trieu Phong, Yoshinori Aono, Takuya Hayashi, Lihua Wang, and Shiho Moriai*  
  Page 100

### Attacks

- Characterizing Promotional Attacks in Mobile App Store
  
  *Bo Sun, Xiapu Luo, Mitsuaki Akiyama, Takuya Watanabe, and Tatsuya Mori*  
  Page 113
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
  Muhamed 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
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