Contents

Encryptions and Signatures

Privacy-Preserving Anomaly Detection Across Multi-domain for Software Defined Networks .................................................. 3  
Huishan Bian, Liehuang Zhu, Meng Shen, Mingzhong Wang, Chang Xu, and Qiongyu Zhang

Distributed Multi-user, Multi-key Searchable Encryptions Resilient Fault Tolerance .......................................................... 17  
Huafei Zhu

Another Look at Aggregate Signatures: Their Capability and Security on Network Graphs .................................................. 32  
Naoto Yanai, Masahiro Mambo, Kazuma Tanaka, Takashi Nishide, and Eiji Okamoto

Universally Composable Oblivious Database in the Presence of Malicious Adversaries .................................................. 49  
Huafei Zhu

Public Key Encryption with Distributed Keyword Search .......................................................... 62  
Veronika Kuchta and Mark Manulis

A Signature Generation Approach Based on Clustering for Polymorphic Worm .................................................. 84  
Jie Wang and Xiaoxian He

Security Model

Computational Soundness of Uniformity Properties for Multi-party Computation Based on LSSS .................................................. 99  
Hui Zhao and Kouichi Sakurai

Attribute-Based Signatures with Controllable Linkability .................................................. 114  
Miguel Urquidi, Dalia Khader, Jean Lancrenon, and Liqun Chen

A Causality-Based Model for Describing the Trustworthiness of a Computing Device .................................................. 130  
Jiun Yi Yap and Allan Tomlinson
Trusted Technologies

An Application-Oriented Efficient Encapsulation System for Trusted Software Development. ............................................ 153
   Zheng Tao, Jun Hu, Jing Zhan, Mo Li, and Chunzi Chen

Research on Trusted Bootstrap Based on the Universal Smart Card. ........ 169
   Lin Yan and Jianbiao Zhang

Efficient Implementation of AND, OR and NOT Operators for ABCs ......... 183
   Antonio de la Piedra

Software and System Security

Application of NTRU Using Group Rings to Partial Decryption Technique ... 203
   Takanori Yasuda, Hiroaki Anada, and Kouichi Sakurai

RbacIP: A RBAC-Based Method for Intercepting and Processing Malicious Applications in Android Platform .................. 214
   Li Lin, Jian Ni, Jian Hu, and Jianbiao Zhang

An Audit Log Protection Mechanism Based on Security Chip ............... 226
   Guan Wang, Ziyi Wang, Jian Sun, and Jun Zhou

Author Index ............................................ 235
Trusted Systems
7th International Conference, INTRUST 2015, Beijing, China, December 7-8, 2015, Revised Selected Papers
Yung, M.; Zhang, J.; Yang, Z. (Eds.)
2016, XII, 235 p. 55 illus., Softcover
ISBN: 978-3-319-31549-2