Contents

Attacks on Data Security Systems

A New Sign-Change Attack on the Montgomery Ladders .......................... 3
Lynn Margaret Batten and Mohammed Khalil Amain

Investigating Cube Attacks on the Authenticated Encryption Stream Cipher
ACORN ................................................................. 15
Md Iftekhar Salam, Harry Bartlett, Ed Dawson, Josef Pieprzyk,
Leonie Simpson, and Kenneth Koon-Ho Wong

Detection of Attacks on Data Security Systems

Investigating Security Vulnerabilities in Modern Vehicle Systems .......... 29
Xi Zheng, Lei Pan, Hongxu Chen, and Peiyin Wang

Tweaking Generic OTR to Avoid Forgery Attacks ............................. 41
Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson,
and Kenneth Koon-Ho Wong

Recent Cyber Security Attacks and Their Mitigation Approaches –
An Overview ..................................................................... 54
Abdullahi Chowdhury

Data Security

Evaluating Entropy Sources for True Random Number Generators
by Collision Counting ................................................................ 69
Maciej Skórski

Enhancement of Sensor Data Transmission by Inference and Efficient
Data Processing ...................................................................... 81
James Jin Kang, Tom H. Luan, and Henry Larkin

An Improved EllipticNet Algorithm for Tate pairing on Weierstrass’
Curves, Faster Point Arithmetic and Pairing on Selmer Curves
and a Note on Double Scalar Multiplication ................................... 93
Srinivasa Rao Subramanya Rao

Inductive Hierarchical Identity Based Key Agreement with Pre-deployment
Interactions (i-H-IB-KA-pdi) ...................................................... 106
Pinaki Sarkar and Morshed Uddin Chowdhury
Data Privacy

Identity-Based Threshold Encryption on Lattices with Application to Searchable Encryption ........................................ 117
  Veronika Kuchta and Olivier Markowitch

Recursive M-ORAM: A Matrix ORAM for Clients with Constrained Storage Space .................................................. 130
  Karin Sumongkayothin, Steven Gordon, Atsuko Miyaji, Chunhua Su, and Komwut Wipusitwarakun

False Signal Injection Attack Detection of Cyber Physical Systems by Event-Triggered Distributed Filtering over Sensor Networks ................................. 142
  Yufeng Lin, Biplob Ray, Dennis Jarvis, and Jia Wang

Mobile Money in the Australasian Region - A Technical Security Perspective .......................................................... 154
  Swathi Parasa and Lynn Margaret Batten

Author Index ................................................................. 163
Applications and Techniques in Information Security
6th International Conference, ATIS 2016, Cairns, QLD, Australia, October 26-28, 2016, Proceedings
Batten, L.; Li, G. (Eds.)
2016, XVI, 163 p. 30 illus., Softcover
ISBN: 978-981-10-2740-6