

Contents

Attacks on Data Security Systems

A New Sign-Change Attack on the Montgomery Ladders	3
<i>Lynn Margaret Batten and Mohammed Khalil Amain</i>	
Investigating Cube Attacks on the Authenticated Encryption Stream Cipher ACORN.	15
<i>Md Iftekhar Salam, Harry Bartlett, Ed Dawson, Josef Pieprzyk, Leonie Simpson, and Kenneth Koon-Ho Wong</i>	

Detection of Attacks on Data Security Systems

Investigating Security Vulnerabilities in Modern Vehicle Systems	29
<i>Xi Zheng, Lei Pan, Hongxu Chen, and Peiyin Wang</i>	
Tweaking Generic OTR to Avoid Forgery Attacks	41
<i>Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, and Kenneth Koon-Ho Wong</i>	
Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview	54
<i>Abdullahi Chowdhury</i>	

Data Security

Evaluating Entropy Sources for True Random Number Generators by Collision Counting	69
<i>Maciej Skórski</i>	
Enhancement of Sensor Data Transmission by Inference and Efficient Data Processing	81
<i>James Jin Kang, Tom H. Luan, and Henry Larkin</i>	
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
<i>Srinivasa Rao Subramanya Rao</i>	
Inductive Hierarchical Identity Based Key Agreement with Pre-deployment Interactions (i-H-IB-KA-pdi).	106
<i>Pinaki Sarkar and Morshed Uddin Chowdhury</i>	

Data Privacy

Identity-Based Threshold Encryption on Lattices with Application to Searchable Encryption	117
<i>Veronika Kuchta and Olivier Markowitch</i>	
Recursive M-ORAM: A Matrix ORAM for Clients with Constrained Storage Space	130
<i>Karin Sumongkayothin, Steven Gordon, Atsuko Miyaji, Chunhua Su, and Komwut Wipusitwarakun</i>	
False Signal Injection Attack Detection of Cyber Physical Systems by Event-Triggered Distributed Filtering over Sensor Networks	142
<i>Yufeng Lin, Biplob Ray, Dennis Jarvis, and Jia Wang</i>	
Mobile Money in the Australasian Region - A Technical Security Perspective	154
<i>Swathi Parasa and Lynn Margaret Batten</i>	
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