Table of Contents

Challenges and Opportunities for Security with Differential Privacy 1
Chris Clifton and Balamurugan Anandan

An Encrypted In-Memory Column-Store: The Onion Selection Problem 14
Florian Kerschbaum, Martin Härterich, Mathias Kohler, Isabelle Hang, Andreas Schaad, Axel Schröpfer, and Walter Tighzert

Risk Aware Approach to Data Confidentiality in Cloud Computing 27
Kerim Yasin Oktay, Vaibhav Khadilkar, Murat Kantarcioglu, and Sharad Mehrotra

Jamming Resistant Schemes for Wireless Communication: A Combinatorial Approach 43
Samiran Bag, Sushmita Ruj, and Bimal Roy

Improved Biometric-Based Three-factor Remote User Authentication Scheme with Key Agreement Using Smart Card 63
Ankita Chaturvedi, Dheerendra Mishra, and Sourav Mukhopadhyay

Signcryption from Randomness Recoverable PKE Revisited 78
Angsuman Das and Avishek Adhikari

Auctions with Rational Adversary 91
Sourya Joyee De and Asim K. Pal

A Framework for Formal Reasoning about Privacy Properties Based on Trust Relationships in Complex Electronic Services 106
Koen Decroix, Jorn Lapon, Bart De Decker, and Vincent Naessens

Correctness Verification in Outsourced Databases: More *Reliable* Fake Tuples Approach 121
Ganugula Umadevi and Ashutosh Saxena

Policy Mining: A Bottom-Up Approach toward a Model Based Firewall Management 133
Safaà Hachana, Frédéric Cuppens, Nora Cuppens-Boulahia, Vijay Atluri, and Stephane Morucci

Secure States *versus* Secure Executions - From Access Control to Flow Control 148
Mathieu Jaume, Radoniaina Andriatsimandefitra, Valérie Viet Triem Tong, and Ludovic Mé

Bibliografische Informationen
http://d-nb.info/1043933603

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Monitoring for Slow Suspicious Activities Using a Target Centric Approach 163
Harsha K. Kalutarage, Siraj A. Shaikh, Qin Zhou, and Anne E. James

RAPID-FeinSPN: A Rapid Prototyping Framework for Feistel and SPN-Based Block Ciphers 169
Ayesha Khalid, Muhammad Hassan, Anupam Chattopadhyay, and Goutam Paul

Simple and Efficient Time-Bound Hierarchical Key Assignment Scheme (Short Paper) 191
Naveen Kumar, Anish Mathuria, and Manik Lal Das

Traitor-Traceable Key Pre-distribution Based on Visual Secret Sharing 199
Sheethal Kumar, Jaipal Pai B.J., Sourav Sen Gupta, and Vigesh R. Ungrapalli

Web Services Based Attacks against Image CAPTCHAs 214
David Lorenzi, Jaideep Vaidya, Shamik Sural, and Vijayalakshmi Atluri

New Long-Term *Glimpse* of RC4 Stream Cipher 230
Subhamoy Maitra and Sourav Sen Gupta

A Voucher Assisted Adaptive Acknowledgement Based Intrusion Detection Protocol for MANETs 239
Soumyadev Maity and R.C. Hansdah

Cryptanalysis of Pairing-Free Identity-Based Authenticated Key Agreement Protocols 247
Dheerendra Mishra and Sourav Mukhopadhyay

Information Theoretical Analysis of Side-Channel Attack 255
Hiroaki Mizuno, Keisuke Iwai, Hidema Tanaka, and Takakazu Kurokawa

Efficient Multi-bit Image Steganography in Spatial Domain 270
Imon Mukherjee and Goutam Paul

Evolutionary Multibit Grouping Steganographic Algorithm 285
Nabanita Mukherjee, Ayon Bhattacharya, and Siddhartha Sekhar Bose

Let the Right One in: Discovering and Mitigating Permission Gaps 297
Beng Heng Ng and Atul Prakash

A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET 314
R.V. Pradweap and R.C. Hansdah

Recipient Anonymous Ciphertext-Policy Attribute Based Encryption . . . 329
Y. Sreenivasa Rao and Ratna Dutta

Error Correction of Partially Exposed RSA Private Keys from MSB Side 345
Santanu Sarkar, Sourav Sen Gupta, and Subhamoy Maitra

Efficient Enforcement of Privacy for Moving Object Trajectories 360
Anuj Shanker Saxena, Vikram Goyal, and Debajyoti Bera

An Administrative Model for Spatio-Temporal Role Based Access Control 375
Manisha Sharma, Shamik Sural, Vijayalakshmi Atluri, and Jaideep Vaidya

A UC-Secure Authenticated Contributory Group Key Exchange Protocol Based on Discrete Logarithm 390
Yasser Sobhdel and Rasool Jalili

Author Index 403