

# Table of Contents

Computational Probabilistic Non-interference .....	1
<i>Michael Backes and Birgit Pfitzmann</i>	
Bit-Slice Auction Circuit .....	24
<i>Kaoru Kurosawa and Wakaha Ogata</i>	
Confidentiality Policies and Their Enforcement for Controlled Query Evaluation .....	39
<i>Joachim Biskup and Piero Bonatti</i>	
Cardinality-Based Inference Control in Sum-Only Data Cubes .....	55
<i>Lingyu Wang, Duminda Wijesekera, and Sushil Jajodia</i>	
Outbound Authentication for Programmable Secure Coprocessors .....	72
<i>Sean W. Smith</i>	
Hamming Weight Attacks on Cryptographic Hardware – Breaking Masking Defense .....	90
<i>Marcin Gomulkiwicz and Mirosław Kutylowski</i>	
A Fully Compliant Research Implementation of the P3P Standard for Privacy Protection: Experiences and Recommendations .....	104
<i>Giles Hogben, Tom Jackson, and Marc Wilikens</i>	
Authentication for Distributed Web Caches .....	126
<i>James Giles, Reiner Sailer, Dinesh Verma, and Suresh Chari</i>	
Analysing a Stream Authentication Protocol Using Model Checking .....	146
<i>Philippa Broadfoot and Gavin Lowe</i>	
Equal To The Task? .....	162
<i>James Heather and Steve Schneider</i>	
TINMAN: A Resource Bound Security Checking System for Mobile Code .....	178
<i>Aloysius K. Mok and Weijiang Yu</i>	
Confidentiality-Preserving Refinement is Compositional – Sometimes .....	194
<i>Thomas Santen, Maritta Heisel, and Andreas Pfitzmann</i>	
Formal Security Analysis with Interacting State Machines .....	212
<i>David von Oheimb and Volkmar Lotz</i>	
Decidability of Safety in Graph-Based Models for Access Control .....	229
<i>Manuel Koch, Luigi V. Mancini, and Francesco Parisi-Presicce</i>	
Inter-Packet Delay Based Correlation for Tracing Encrypted Connections through Stepping Stones .....	244
<i>Xinyuan Wang, Douglas S. Reeves, and S. Felix Wu</i>	

Learning Fingerprints for a Database Intrusion Detection System ..... 264  
*Sin Yeung Lee, Wai Lup Low, and Pei Yuen Wong*

**Author Index** ..... 281