

Table of Contents

Authentication Mechanisms

Secret Handshake Scheme with Request-Based-Revealing	1
<i>Yutaka Kawai and Noboru Kunihiro</i>	
Password-Based Signatures	17
<i>Kristian Gjøsteen and Øystein Thuen</i>	
Isolating Partial Information of Indistinguishable Encryptions	34
<i>Jean Lancrenon and Roland Gillard</i>	

Invited Paper

A Universal Client-Based Identity Management Tool	49
<i>Haitham S. Al-Sinani and Chris J. Mitchell</i>	

Privacy Preserving Techniques

Design and Evaluation of a Privacy-Preserving Architecture for Vehicle-to-Grid Interaction	75
<i>Mark Stegelmann and Dogan Kesdogan</i>	
Insider Attacks and Privacy of RFID Protocols	91
<i>Ton van Deursen and Saša Radomirović</i>	
Cell-Based Roadpricing	106
<i>Flavio D. Garcia, Eric R. Verheul, and Bart Jacobs</i>	

Invited Paper

Ballot Aggregation and Mixnet Based Open-Audit Elections (Extended Abstract)	123
<i>Olivier Pereira</i>	

Invited Paper

PKI as Part of an Integrated Risk Management Strategy for Web Security	128
<i>Peter Gutmann</i>	

PKI Applications

A PKI-Based Mobile Banking Demonstrator..... 147
 Gauthier Van Damme, Nicolas Luyckx, and Karel Wouters

Certification Validation: Back to the Past 159
 Moez Ben MBarka and Julien P. Stern

Secure Applications

A Hijacker’s Guide to the LPC Bus 176
 Johannes Winter and Kurt Dietrich

Secure Event Logging in Sensor Networks 194
 An Braeken, Antonio De La Piedro, and Karel Wouters

Author Index 209