

Table of Contents

Mobility

On the Unobservability of a Trust Relation in Mobile Ad Hoc Networks	1
<i>Olivier Heen, Gilles Guette, and Thomas Genet</i>	
A Mechanism to Avoid Collusion Attacks Based on Code Passing in Mobile Agent Systems	12
<i>Marc Jaimez, Oscar Esparza, Jose L. Muñoz, Juan J. Alins-Delgado, and Jorge Mata-Díaz</i>	
Privacy-Aware Location Database Service for Granular Queries	28
<i>Shinsaku Kiyomoto, Keith M. Martin, and Kazuhide Fukushima</i>	

Attacks and Secure Implementations

Algebraic Attacks on RFID Protocols	38
<i>Ton van Deursen and Saša Radomirović</i>	
Anti-counterfeiting Using Memory Spots	52
<i>Helen Balinsky, Edward McDonnell, Liqun Chen, and Keith Harrison</i>	
On Second-Order Fault Analysis Resistance for CRT-RSA Implementations	68
<i>Emmanuelle Dottax, Christophe Giraud, Matthieu Rivain, and Yannick Sierra</i>	

Performance and Security

Measurement Analysis When Benchmarking Java Card Platforms	84
<i>Pierre Paradinas, Julien Cordry, and Samia Bouzefrane</i>	
Performance Issues of Selective Disclosure and Blinded Issuing Protocols on Java Card	95
<i>Hendrik Tews and Bart Jacobs</i>	
Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks	112
<i>Christian Lederer, Roland Mader, Manuel Koschuch, Johann Großschädl, Alexander Szekeley, and Stefan Tillich</i>	

Cryptography

Key Management Schemes for Peer-to-Peer Multimedia Streaming
Overlay Networks 128
 J.A.M. Naranjo, J.A. López-Ramos, and L.G. Casado

Ultra-Lightweight Key Predistribution in Wireless Sensor Networks for
Monitoring Linear Infrastructure 143
 Keith M. Martin and Maura B. Paterson

PKIX Certificate Status in Hybrid MANETs 153
 *Jose L. Muñoz, Oscar Esparza, Carlos Gañán, and
 Javier Parra-Arnau*

Author Index 167