

Contents

NFC and Mobile Security

Deploying OSK on Low-Resource Mobile Devices.	3
<i>Gildas Avoine, Muhammed Ali Bingöl, Xavier Carpent, and Süleyman Kardaş</i>	
Is NFC a Better Option Instead of EPC Gen-2 in Safe Medication of Inpatients	19
<i>Mehmet Hilal Özcanhan, Gökhan Dalkılıç, and Semih Utku</i>	
Rights Management with NFC Smartphones and Electronic ID Cards: A Proof of Concept for Modern Car Sharing	34
<i>Timo Kasper, Alexander Kühn, David Oswald, Christian Zenger, and Christof Paar</i>	

Protocols and Attacks

Desynchronization and Traceability Attacks on RIPTA-DA Protocol	57
<i>Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani, and Somitra Kumar Sanadhya</i>	
Long Distance Relay Attack.	69
<i>Luigi Sportiello and Andrea Ciardulli</i>	
On the Security of Two RFID Mutual Authentication Protocols	86
<i>Seyed Farhad Aghili, Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani, and Somitra Kumar Sanadhya</i>	

RFID Hardware

Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures	103
<i>Lejla Batina, Amitabh Das, Barış Ege, Elif Bilge Kavun, Nele Mentens, Christof Paar, Ingrid Verbauwhede, and Tolga Yalçın</i>	
An Improved Hardware Implementation of the Quark Hash Function	113
<i>Shohreh Sharif Mansouri and Elena Dubrova</i>	

Analyzing Side-Channel Leakage of RFID-Suitable Lightweight
ECC Hardware 128
 Erich Wenger, Thomas Korak, and Mario Kirschbaum

Implementations

Energy-Architecture Tuning for ECC-Based RFID Tags 147
 Deepak Mane and Patrick Schaumont

Speed and Size-Optimized Implementations of the PRESENT
Cipher for Tiny AVR Devices 161
 Konstantinos Papagiannopoulos and Aram Versteegen

Author Index 177