

# Contents

## **NFC and Mobile Security**

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

## **Protocols and Attacks**

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

## **RFID Hardware**

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

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



<http://www.springer.com/978-3-642-41331-5>

Radio Frequency Identification: Security and Privacy  
Issues

Security and Privacy Issues 9th International Workshop,  
RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised  
Selected Papers

Hutter, M.; Schmidt, J.-M. (Eds.)

2013, XIV, 177 p. 59 illus., Softcover

ISBN: 978-3-642-41331-5