

# Contents

## NFC and Mobile Security

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

## Protocols and Attacks

|   |    |
|---|----|
| Desynchronization and Traceability Attacks on RIPTA-DA Protocol . . . . .   | 57 |
| <i>Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani,<br/>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,<br/>Masoumeh Safkhani, and Somitra Kumar Sanadhya</i> |    |

## RFID Hardware

|   |     |
|---|-----|
| Dietary Recommendations for Lightweight Block Ciphers: Power,<br>Energy and Area Analysis of Recently Developed Architectures . . . . . | 103 |
| <i>Lejla Batina, Amitabh Das, Barış Ege, Elif Bilge Kavun, Nele Mentens,<br/>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<br>ECC Hardware . . . . . | 128 |
| <i>Erich Wenger, Thomas Korak, and Mario Kirschbaum</i>                               |     |

## **Implementations**

|  |     |
|--|-----|
| Energy-Architecture Tuning for ECC-Based RFID Tags . . . . . | 147 |
| <i>Deepak Mane and Patrick Schaumont</i>                     |     |

|  |     |
|--|-----|
| Speed and Size-Optimized Implementations of the PRESENT<br>Cipher for Tiny AVR Devices . . . . . | 161 |
| <i>Konstantinos Papagiannopoulos and Aram Versteegen</i>   |     |

|                               |     |
|-------------------------------|-----|
| <b>Author Index</b> . . . . . | 177 |
|-------------------------------|-----|

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