

Contents

Lightweight Authentication Protocols on Ultra-Constrained RFIDs - Myths and Facts	1
<i>Frederik Armknecht, Matthias Hamann, and Vasily Mikhalev</i>	
High-Speed Dating Privacy-Preserving Attribute Matching for RFID	19
<i>Lejla Batina, Jens Hermans, Jaap-Henk Hoepman, and Anna Krasnova</i>	
Massively Parallel Identification of Privacy-Preserving Vehicle RFID Tags. . . .	36
<i>Rui Figueiredo, André Zúquete, and Tomás Oliveira e Silva</i>	
PIONEER—a Prototype for the Internet of Things Based on an Extendable EPC Gen2 RFID Tag	54
<i>Hannes Gross, Erich Wenger, Honorio Martín, and Michael Hutter</i>	
SeAK: Secure Authentication and Key Generation Protocol Based on Dual Antennas for Wireless Body Area Networks.	74
<i>Chitra Javali, Girish Revadigar, Lavy Libman, and Sanjay Jha</i>	
Cryptanalysis of SIMON Variants with Connections	90
<i>Javad Alizadeh, Hoda A. Alkhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, Martin M. Lauridsen, and Somitra Kumar Sanadhya</i>	
Privacy-Preserving Authorized RFID Authentication Protocols	108
<i>Nan Li, Yi Mu, Willy Susilo, Fuchun Guo, and Vijay Varadharajan</i>	
Energy Budget Analysis for Signature Protocols on a Self-powered Wireless Sensor Node	123
<i>Krishna Pabbuleti, Deepak Mane, and Patrick Schaumont</i>	
High Throughput in Slices: The Case of PRESENT, PRINCE and KATAN64 Ciphers	137
<i>Kostas Papapagiannopoulos</i>	
Curved Tags – A Low-Resource ECDSA Implementation Tailored for RFID . . .	156
<i>Peter Pessl and Michael Hutter</i>	
ePassport: Side Channel in the Basic Access Control.	173
<i>Luigi Sportiello</i>	

A Low Area Probing Detector for Power Efficient Security ICs 185
Michael Weiner, Salvador Manich, and Georg Sigl

Non-Linear Collision Analysis 198
Xin Ye, Cong Chen, and Thomas Eisenbarth

Author Index 215

Radio Frequency Identification: Security and Privacy
Issues

10th International Workshop, RFIDSec 2014, Oxford, UK,
July 21-23, 2014, Revised Selected Papers

Saxena, N.; Sadeghi, A.-R. (Eds.)

2014, VIII, 215 p. 62 illus., Softcover

ISBN: 978-3-319-13065-1