

# Contents

## Protocols

Security Analysis of Niu <i>et al.</i> Authentication and Ownership Management Protocol . . . . .	3
<i>Masoumeh Safkhani, Hoda Jannati, and Nasour Bagheri</i>	
PTSLP: Position Tracking Based Source Location Privacy for Wireless Sensor Networks. . . . .	17
<i>Hao Wang, Guangjie Han, Chunsheng Zhu, and Sammy Chan</i>	
A Robust Authentication Protocol with Privacy Protection for Wireless Sensor Networks. . . . .	30
<i>Xiong Li, Jianwei Niu, and Kim-Kwang Raymond Choo</i>	

## Side Channel and Hardware

Energy Optimization of Unrolled Block Ciphers Using Combinational Checkpointing . . . . .	47
<i>Siva Nishok Dhanuskodi and Daniel Holcomb</i>	
LDA-Based Clustering as a Side-Channel Distinguisher . . . . .	62
<i>Rauf Mahmudlu, Valentina Banciu, Lejla Batina, and Ileana Buhan</i>	
Efficient Implementation of Ring-LWE Encryption on High-End IoT Platform. . . . .	76
<i>Zhe Liu, Reza Azarderakhsh, Howon Kim, and Hwajeong Seo</i>	
Side-Channel Analysis of Lightweight Ciphers: Does Lightweight Equal Easy? . . . . .	91
<i>Annelie Heuser, Stjepan Picek, Sylvain Guilley, and Nele Mentens</i>	

## Cards and Tokens

Enhancing EMV Tokenisation with Dynamic Transaction Tokens . . . . .	107
<i>Danushka Jayasinghe, Konstantinos Markantonakis, Raja Naeem Akram, and Keith Mayes</i>	
Bias in the Mifare DESFire EV1 TRNG . . . . .	123
<i>Darren Hurley-Smith and Julio Hernandez-Castro</i>	

**Proximity**

Optimality Results on the Security of Lookup-Based Protocols . . . . .	137
<i>Sjouke Mauw, Jorge Toro-Pozo, and Rolando Trujillo-Rasua</i>	
Towards Quantum Distance Bounding Protocols . . . . .	151
<i>Aysajan Abidin, Eduard Marin, Dave Singelée, and Bart Preneel</i>	
Matching in Proximity Authentication and Mobile Payment EcoSystem: What Are We Missing? . . . . .	163
<i>Yunhui Zhuang, Alvin Chung Man Leung, and James Hughes</i>	

**Communication**

$\mu$ Proxy: A Hardware Relay for Anonymous and Secure Internet Access. . . . .	175
<i>David Cox and David Oswald</i>	
Self-jamming Audio Channels: Investigating the Feasibility of Perceiving Overshadowing Attacks . . . . .	188
<i>Qiao Hu and Gerhard Hancke</i>	
<b>Author Index</b> . . . . .	205

Radio Frequency Identification and IoT Security  
12th International Workshop, RFIDSec 2016, Hong  
Kong, China, November 30 -- December 2, 2016,  
Revised Selected Papers  
Hancke, G.P.; Markantonakis, K. (Eds.)  
2017, X, 205 p. 56 illus., Softcover  
ISBN: 978-3-319-62023-7