

# Contents

## Cryptanalysis

Faster Key Recovery Attack on Round-Reduced PRINCE . . . . .	3
<i>Shahram Rasoolzadeh and Håvard Raddum</i>	
Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited . . . . .	18
<i>Cihangir Tezcan, Galip Oral Okan, Asuman Şenol, Erol Doğan, Furkan Yücebaş, and Nazife Baykal</i>	
Impossible Differential Cryptanalysis of 16/18-Round Khudra . . . . .	33
<i>Ferhat Karakoç, Öznur Mut Sağdıçoğlu, Mehmet Emin Gönen, and Oğuzhan Ersoy</i>	
Distinguishing Attacks on (Ultra-)Lightweight WG Ciphers . . . . .	45
<i>Mabin Joseph, Gautham Sekar, and R. Balasubramanian</i>	
Cryptanalysis of QTL Block Cipher . . . . .	60
<i>Mustafa Çoban, Ferhat Karakoç, and Mehmet Özen</i>	
A Brief Comparison of SIMON and SIMECK . . . . .	69
<i>Stefan Kölbl and Arnab Roy</i>	

## Lightweight Designs and Implementations

Bitsliced Masking and ARM: Friends or Foes? . . . . .	91
<i>Wouter de Groot, Kostas Papagiannopoulos, Antonio de La Piedra, Erik Schneider, and Lejla Batina</i>	
Classification of $6 \times 6$ S-boxes Obtained by Concatenation of RSSBs . . . . .	110
<i>Selçuk Kavut and Sevdnur Baloğlu</i>	
Concealing KETJE: A Lightweight PUF-Based Privacy Preserving Authentication Protocol . . . . .	128
<i>Gerben Geltink</i>	
Author Index . . . . .	149

Lightweight Cryptography for Security and Privacy  
5th International Workshop, LightSec 2016, Aksaray,  
Turkey, September 21-22, 2016, Revised Selected  
Papers  
Bogdanov, A. (Ed.)  
2017, VII, 149 p. 34 illus., Softcover  
ISBN: 978-3-319-55713-7