

# Contents

## Efficient Implementations and Designs

The SIMON and SPECK Block Ciphers on AVR 8-Bit Microcontrollers. . . . .	3
<i>Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers</i>	
The Multiplicative Complexity of Boolean Functions on Four and Five Variables . . . . .	21
<i>Meltem Turan Sönmez and René Peralta</i>	
A Flexible and Compact Hardware Architecture for the SIMON Block Cipher . . . . .	34
<i>Ege Gulcan, Aydın Aysu, and Patrick Schaumont</i>	
AES Smaller Than S-Box: Minimalism in Software Design on Low End Microcontrollers . . . . .	51
<i>Mitsuru Matsui and Yumiko Murakami</i>	

## Attacks

Differential Factors: Improved Attacks on SERPENT . . . . .	69
<i>Cihangir Tezcan and Ferruh Özbudak</i>	
Ciphertext-Only Fault Attacks on PRESENT . . . . .	85
<i>Fabrizio De Santis, Oscar M. Guillen, Ermin Sakic, and Georg Sigl</i>	
Relating Undisturbed Bits to Other Properties of Substitution Boxes . . . . .	109
<i>Rusydi H. Makarim and Cihangir Tezcan</i>	
Differential Sieving for 2-Step Matching Meet-in-the-Middle Attack with Application to LBlock . . . . .	126
<i>Riham AlTawy and Amr M. Youssef</i>	
Match Box Meet-in-the-Middle Attacks on the SIMON Family of Block Ciphers. . . . .	140
<i>Ling Song, Lei Hu, Bingke Ma, and Danping Shi</i>	

## Protocols

A Provably Secure Offline RFID Yoking-Proof Protocol with Anonymity . . .	155
<i>Daisuke Moriyama</i>	

Author Index . . . . .	169
------------------------	-----

Lightweight Cryptography for Security and Privacy  
Third International Workshop, LightSec 2014, Istanbul,  
Turkey, September 1-2, 2014, Revised Selected Papers  
Eisenbarth, Th.; Öztürk, E. (Eds.)  
2015, XIII, 169 p. 33 illus., Softcover  
ISBN: 978-3-319-16362-8