Contents

Efficient Implementations and Designs

The Simon and Speck Block Ciphers on AVR 8-Bit Microcontrollers . . . . . . . 3
Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark,
Bryan Weeks, and Louis Wingers

The Multiplicative Complexity of Boolean Functions on Four
and Five Variables ................................................................. 21
Meltem Turan Sönmez and René Peralta

A Flexible and Compact Hardware Architecture for the SIMON
Block Cipher ........................................................................ 34
Ege Gulcan, Aydin Aysu, and Patrick Schaumont

AES Smaller Than S-Box: Minimalism in Software Design
on Low End Microcontrollers ................................................. 51
Mitsuru Matsui and Yumiko Murakami

Attacks

Differential Factors: Improved Attacks on SERPENT ..................... 69
Cihangir Tezcan and Ferruh Özbudak

Ciphertext-Only Fault Attacks on PRESENT ............................. 85
Fabrizio De Santis, Oscar M. Guillen, Ermin Sakic, and Georg Sigl

Relating Undisturbed Bits to Other Properties of Substitution Boxes .... 109
Rusydi H. Makarim and Cihangir Tezcan

Differential Sieving for 2-Step Matching Meet-in-the-Middle Attack
with Application to LBlock ..................................................... 126
Riham Altawy and Amr M. Youssef

Match Box Meet-in-the-Middle Attacks on the SIMON Family
of Block Ciphers ..................................................................... 140
Ling Song, Lei Hu, Bingke Ma, and Danping Shi

Protocols

A Provably Secure Offline RFID Yoking-Proof Protocol with Anonymity . . 155
Daisuke Moriyama

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