

Contents

Cryptanalysis

Meet-in-the-Middle Attacks on Reduced Round Piccolo	3
<i>Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef</i>	
Differential Factors Revisited: Corrected Attacks on PRESENT and SERPENT	21
<i>Cihangir Tezcan</i>	

Lightweight Constructions

A Light-Weight Group Signature Scheme with Time-Token Dependent Linking	37
<i>Keita Emura and Takuya Hayashi</i>	
RoadRunner: A Small and Fast Bitslice Block Cipher for Low Cost 8-Bit Processors	58
<i>Adnan Baysal and Sühap Şahin</i>	
PUF-Based Mutual Multifactor Entity and Transaction Authentication for Secure Banking.	77
<i>Amanda C. Davi Resende, Karina Mochetti, and Diego F. Aranha</i>	
On Lightweight Security Enforcement in Cyber-Physical Systems	97
<i>Yanjiang Yang, Jiqiang Lu, Kim-Kwang Raymond Choo, and Joseph K. Liu</i>	

Implementation Challenges

Fast Software Implementation of QUARK on a 32-Bit Architecture	115
<i>Roberto Cabral and Julio López</i>	
Single-Cycle Implementations of Block Ciphers	131
<i>Pieter Maene and Ingrid Verbauwhede</i>	
Improved Power Analysis on Unrolled Architecture and Its Application to PRINCE Block Cipher.	148
<i>Ville Yli-Mäyry, Naofumi Homma, and Takafumi Aoki</i>	

Author Index	165
-------------------------------	-----

Lightweight Cryptography for Security and Privacy
4th International Workshop, LightSec 2015, Bochum,
Germany, September 10-11, 2015, Revised Selected
Papers

Güneysu, T.; Leander, G.; Moradi, A. (Eds.)

2016, IX, 165 p. 44 illus. in color., Softcover

ISBN: 978-3-319-29077-5