

# Contents

## Symmetric Key Cryptography

Boolean Functions with Maximum Algebraic Immunity Based on Properties of Punctured Reed–Muller Codes . . . . .	3
<i>Konstantinos Limniotis and Nicholas Kolokotronis</i>	
Results on Characterizations of Plateaued Functions in Arbitrary Characteristic . . . . .	17
<i>Sihem Mesnager, Ferruh Özbudak, and Ahmet Sinak</i>	
Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm . . . . .	31
<i>Georgi Ivanov, Nikolay Nikolov, and Svetla Nikova</i>	

## Cryptanalysis

Analysis of the Authenticated Cipher MORUS (v1). . . . .	45
<i>Aleksandra Mileva, Vesna Dimitrova, and Vesselin Velichkov</i>	
Linear Cryptanalysis and Modified DES with Embedded Parity Check in the S-boxes . . . . .	60
<i>Yuri Borissov, Peter Boyvalenkov, and Robert Tsenkov</i>	
Time-Advantage Ratios Under Simple Transformations: Applications in Cryptography . . . . .	79
<i>Maciej Skórski</i>	

## Security and Protocols

Synchronous Universally Composable Computer Networks . . . . .	95
<i>Dirk Achenbach, Jörn Müller-Quade, and Jochen Rill</i>	
Key-Policy Attribute-Based Encryption for General Boolean Circuits from Secret Sharing and Multi-linear Maps . . . . .	112
<i>Constantin Cătălin Drăgan and Ferucio Laurențiu Țiplea</i>	
Closing the Gap: A Universal Privacy Framework for Outsourced Data . . . . .	134
<i>Dirk Achenbach, Matthias Huber, Jörn Müller-Quade, and Jochen Rill</i>	

**Implementation and Verifiable Encryption**

On the Efficiency of Polynomial Multiplication for Lattice-Based Cryptography on GPUs Using CUDA . . . . .	155
<i>Sedat Akleylek, Özgür Dağdelen, and Zaliha Yüce Tok</i>	
cuHE: A Homomorphic Encryption Accelerator Library. . . . .	169
<i>Wei Dai and Berk Sunar</i>	
Extended Functionality in Verifiable Searchable Encryption . . . . .	187
<i>James Alderman, Christian Janson, Keith M. Martin, and Sarah Louise Renwick</i>	
<b>Author Index</b> . . . . .	207

Cryptography and Information Security in the Balkans  
Second International Conference, BalkanCryptSec  
2015, Koper, Slovenia, September 3-4, 2015, Revised  
Selected Papers

Pasalic, E.; Knudsen, L.R. (Eds.)

2016, VIII, 207 p. 19 illus., Softcover

ISBN: 978-3-319-29171-0