

# Contents

## Invited Paper

On Existence (Based on an Arithmetical Problem) and Constructions of Bent Functions . . . . .	3
<i>Sihem Mesnager, Gérard Cohen, and David Madore</i>	

## Best Paper Award

Security Against Related Randomness Attacks via Reconstructive Extractors . . . . .	23
<i>Kenneth G. Paterson, Jacob C.N. Schuldt, Dale L. Sibborn, and Hoeteck Wee</i>	

## Authentication

MI-T-HFE, A New Multivariate Signature Scheme . . . . .	43
<i>Wenbin Zhang and Chik How Tan</i>	
A New Approach to Efficient Revocable Attribute-Based Anonymous Credentials . . . . .	57
<i>David Derler, Christian Hanser, and Daniel Slamanig</i>	

## Symmetric Cryptography

Tweak-Length Extension for Tweakable Blockciphers . . . . .	77
<i>Kazuhiko Minematsu and Tetsu Iwata</i>	
Rogue Decryption Failures: Reconciling AE Robustness Notions . . . . .	94
<i>Guy Barwell, Daniel Page, and Martijn Stam</i>	
Robust Authenticated Encryption and the Limits of Symmetric Cryptography . . . . .	112
<i>Christian Badertscher, Christian Matt, Ueli Maurer, Phillip Rogaway, and Björn Tackmann</i>	

## 2-Party Computation

A Compiler of Two-Party Protocols for Composable and Game-Theoretic Security, and Its Application to Oblivious Transfer . . . . .	133
<i>Shota Goto and Junji Shikata</i>	

Zero-Knowledge Interactive Proof Systems for New Lattice Problems . . . . .	152
<i>Claude Crépeau and Raza Ali Kazmi</i>	

**Codes**

Soft Distance Metric Decoding of Polar Codes . . . . .	173
<i>Monica C. Liberatori, Leonardo J. Arnone, Jorge Castiñeira Moreira, and Patrick G. Farrell</i>	
On the Doubly Sparse Compressed Sensing Problem. . . . .	184
<i>Grigory Kabatiansky, Serge Vlăduț, and Cedric Tavernier</i>	
Codes of Length 2 Correcting Single Errors of Limited Size . . . . .	190
<i>Torleiv Kløve</i>	

**Boolean Functions**

Bent and Semi-bent Functions via Linear Translators. . . . .	205
<i>Neşe Koçak, Sihem Mesnager, and Ferruh Özbudak</i>	
Comparison of Cube Attacks Over Different Vector Spaces . . . . .	225
<i>Richard Winter, Ana Salagean, and Raphael C.-W. Phan</i>	
On the Diffusion Property of Iterated Functions . . . . .	239
<i>Jian Liu, Sihem Mesnager, and Lusheng Chen</i>	

**Information Theory**

Shannon Entropy Versus Renyi Entropy from a Cryptographic Viewpoint . . .	257
<i>Maciej Skórski</i>	

**Leakage Resilience**

Continuous After-the-Fact Leakage-Resilient eCK-Secure Key Exchange . . . .	277
<i>Janaka Alawattugoda, Douglas Stebila, and Colin Boyd</i>	
A Leakage Resilient MAC . . . . .	295
<i>Daniel P. Martin, Elisabeth Oswald, Martijn Stam, and Marcin Wójcik</i>	
Leakage-Resilient Identification Schemes from Zero-Knowledge Proofs of Storage . . . . .	311
<i>Giuseppe Ateniese, Antonio Faonio, and Seny Kamara</i>	

<b>Author Index</b> . . . . .	329
-------------------------------	-----

Cryptography and Coding

15th IMA International Conference, IMACC 2015, Oxford,

UK, December 15-17, 2015. Proceedings

Groth, J. (Ed.)

2015, X, 329 p. 42 illus. in color., Softcover

ISBN: 978-3-319-27238-2