

Contents

Designs

Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes	3
<i>Daniel Augot and Matthieu Finiasz</i>	
LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations	18
<i>Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici</i>	
SPRING: Fast Pseudorandom Functions from Rounded Ring Products.	38
<i>Abhishek Banerjee, Hai Brenner, Gaëtan Leurent, Chris Peikert, and Alon Rosen</i>	

Cryptanalysis I

Match Box Meet-in-the-Middle Attack Against KATAN	61
<i>Thomas Fuhr and Brice Minaud</i>	
Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64	82
<i>Léo Perrin and Dmitry Khovratovich</i>	
Improved All-Subkeys Recovery Attacks on FOX, KATAN and SHACAL-2 Block Ciphers	104
<i>Takanori Isobe and Kyoji Shibutani</i>	
Improved Single-Key Attacks on 9-Round AES-192/256	127
<i>Leibo Li, Keting Jia, and Xiaoyun Wang</i>	

Authenticated Encryption

CLOC: Authenticated Encryption for Short Input	149
<i>Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, and Sumio Morioka</i>	
APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography.	168
<i>Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda</i>	

COBRA: A Parallelizable Authenticated Online Cipher Without Block Cipher Inverse	187
<i>Elena Andreeva, Atul Luykx, Bart Mennink, and Kan Yasuda</i>	
Pipelineable On-line Encryption	205
<i>Farzaneh Abed, Scott Fluhrer, Christian Forler, Eik List, Stefan Lucks, David McGrew, and Jakob Wenzel</i>	
Cryptanalysis of FIDES	224
<i>Itai Dinur and J��r��my Jean</i>	
Foundations and Theory	
Security Analysis of Key-Alternating Feistel Ciphers	243
<i>Rodolphe Lampe and Yannick Seurin</i>	
The Related-Key Analysis of Feistel Constructions	265
<i>Manuel Barbosa and Pooya Farshim</i>	
The Indistinguishability of the XOR of k Permutations	285
<i>Beno��t Cogliati, Rodolphe Lampe, and Jacques Patarin</i>	
Impact of ANSI X9.24-1:2009 Key Check Value on ISO/IEC 9797-1:2011 MACs	303
<i>Tetsu Iwata and Lei Wang</i>	
Stream Ciphers	
Plaintext Recovery Attacks Against WPA/TKIP	325
<i>Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt</i>	
Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA	350
<i>Sourav Sen Gupta, Subhamoy Maitra, Willi Meier, Goutam Paul, and Santanu Sarkar</i>	
Cryptanalysis II	
Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro	373
<i>Hadi Soleimany</i>	
Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64	390
<i>Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir</i>	

Differential-Linear Cryptanalysis Revisited.	411
<i>Céline Blondeau, Gregor Leander, and Kaisa Nyberg</i>	
Improved Slender-Set Linear Cryptanalysis.	431
<i>Guo-Qiang Liu, Chen-Hui Jin, and Chuan-Da Qi</i>	
Cryptanalysis of KLEIN.	451
<i>Virginie Lallemand and María Naya-Plasencia</i>	
Hash Functions	
Branching Heuristics in Differential Collision Search with Applications to SHA-512	473
<i>Maria Eichlseder, Florian Mendel, and Martin Schläffer</i>	
On the Minimum Number of Multiplications Necessary for Universal Hash Functions.	489
<i>Mridul Nandi</i>	
Collision Attack on 5 Rounds of Grøstl.	509
<i>Florian Mendel, Vincent Rijmen, and Martin Schläffer</i>	
Cryptanalysis III	
Differential Cryptanalysis of Round-Reduced SIMON and SPECK.	525
<i>Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel</i>	
Differential Analysis of Block Ciphers SIMON and SPECK.	546
<i>Alex Biryukov, Arnab Roy, and Vesselin Velichkov</i>	
Equivalent Key Recovery Attacks Against HMAC and NMAC with Whirlpool Reduced to 7 Rounds	571
<i>Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang, and Long Wen</i>	
Multiple Differential Cryptanalysis of Round-Reduced PRINCE	591
<i>Anne Canteaut, Thomas Fuhr, Henri Gilbert, María Naya-Plasencia, and Jean-René Reinhard</i>	
Advanced Constructions	
Efficient Fuzzy Search on Encrypted Data	613
<i>Alexandra Boldyreva and Nathan Chenette</i>	
Author Index	635

Fast Software Encryption

21st International Workshop, FSE 2014, London, UK,

March 3-5, 2014. Revised Selected Papers

Cid, C.; Rechberger, C. (Eds.)

2015, XI, 636 p. 155 illus., Softcover

ISBN: 978-3-662-46705-3