Contents

Designs

Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes 3
Daniel Augot and Matthieu Finiasz

LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations 18
Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici

SPRING: Fast Pseudorandom Functions from Rounded Ring Products. 38
Abhishek Banerjee, Hai Brenner, Gaëtan Leurent, Chris Peikert, and Alon Rosen

Cryptanalysis I

Match Box Meet-in-the-Middle Attack Against KATAN 61
Thomas Fuhr and Brice Minaud

Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64 82
Léo Perrin and Dmitry Khovratovich

Improved All-Subkeys Recovery Attacks on FOX, KATAN and SHACAL-2 Block Ciphers 104
Takanori Isobe and Kyoji Shibutani

Improved Single-Key Attacks on 9-Round AES-192/256 127
Leibo Li, Keting Jia, and Xiaoyun Wang

Authenticated Encryption

CLOC: Authenticated Encryption for Short Input 149
Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, and Sumio Morioka

APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography. 168
Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda

Bibliografische Informationen
http://d-nb.info/1067308342

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

COBRA: A Parallelizable Authenticated Online Cipher Without Block Cipher Inverse 187
Elena Andreeva, Atul Luykx, Bart Mennink, and Kan Yasuda

Pipelineable On-line Encryption 205
Farzaneh Abed, Scott Fluhrer, Christian Forler, Eik List, Stefan Lucks, David McGrew, and Jakob Wenzel

Cryptanalysis of FIDES 224
Itai Dinur and Jérémy Jean

Foundations and Theory

Security Analysis of Key-Alternating Feistel Ciphers 243
Rodolphe Lampe and Yannick Seurin

The Related-Key Analysis of Feistel Constructions 265
Manuel Barbosa and Pooya Farshim

The Indistinguishability of the XOR of k Permutations 285
Benoit Cogliati, Rodolphe Lampe, and Jacques Patarin

Impact of ANSI X9.24-1:2009 Key Check Value on ISO/IEC 9797-1:2011 MACs 303
Tetsu Iwata and Lei Wang

Stream Ciphers

Plaintext Recovery Attacks Against WPA/TKIP 325
Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt

Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA 350
Sourav Sen Gupta, Subhamoy Maitra, Willi Meier, Goutam Paul, and Santanu Sarkar

Cryptanalysis II

Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro. 373
Hadi Soleimany

Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64 390
Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir

Differential-Linear Cryptanalysis Revisited 411
Céline Blondeau, Gregor Leander, and Kaisa Nyberg

Improved Slender-Set Linear Cryptanalysis. 431
Guo-Qiang Liu, Chen-Hui Jin, and Chuan-Da Qi

Cryptanalysis of KLEIN. 451
Virginie Lallemand and María Naya-Plasencia

Hash Functions

Branching Heuristics in Differential Collision Search with Applications to SHA-512 473
Maria Eichlseder, Florian Mendel, and Martin Schläffer

On the Minimum Number of Multiplications Necessary for Universal Hash Functions 489
Mridul Nandi

Collision Attack on 5 Rounds of `Grøstl` 509
Florian Mendel, Vincent Rijmen, and Martin Schläffer

Cryptanalysis III

Differential Cryptanalysis of Round-Reduced SIMON and SPECK 525
Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel

Differential Analysis of Block Ciphers SIMON and SPECK. 546
Alex Biryukov, Arnab Roy, and Vesselin Velichkov

Equivalent Key Recovery Attacks Against `HMAC` and `NMAC` with `Whirlpool` Reduced to 7 Rounds 571
Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang, and Long Wen

Multiple Differential Cryptanalysis of Round-Reduced PRINCE 591
Anne Canteaut, Thomas Fuhr, Henri Gilbert, María Naya-Plasencia, and Jean-René Reinhard

Advanced Constructions

Efficient Fuzzy Search on Encrypted Data 613
Alexandra Boldyreva and Nathan Chenette

Author Index 635