

Contents

Operating Modes

New Bounds for Keyed Sponges with Extendable Output: Independence Between Capacity and Message Length	3
<i>Yusuke Naito and Kan Yasuda</i>	
RIV for Robust Authenticated Encryption	23
<i>Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel</i>	
A MAC Mode for Lightweight Block Ciphers	43
<i>Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda</i>	

Stream-Cipher Cryptanalysis

Cryptanalysis of the Full Spritz Stream Cipher	63
<i>Subhadeep Banik and Takanori Isobe</i>	
Attacks Against Filter Generators Exploiting Monomial Mappings	78
<i>Anne Canteaut and Yann Rotella</i>	

Components

Lightweight MDS Generalized Circulant Matrices	101
<i>Meicheng Liu and Siang Meng Sim</i>	
On the Construction of Lightweight Circulant Involutory MDS Matrices	121
<i>Yongqiang Li and Mingsheng Wang</i>	
Optimizing S-Box Implementations for Several Criteria Using SAT Solvers . . .	140
<i>Ko Stoffelen</i>	

Side-Channels and Implementations

Verifiable Side-Channel Security of Cryptographic Implementations: Constant-Time MEE-CBC	163
<i>José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and François Dupressoir</i>	
White-Box Cryptography in the Gray Box: – A Hardware Implementation and its Side Channels –	185
<i>Pascal Sasdrich, Amir Moradi, and Tim Güneysu</i>	

Detecting Flawed Masking Schemes with Leakage Detection Tests	204
<i>Oscar Reparaz</i>	

There Is Wisdom in Harnessing the Strengths of Your Enemy: Customized Encoding to Thwart Side-Channel Attacks	223
<i>Housseem Maghrebi, Victor Servant, and Julien Bringer</i>	

Automated Tools for Cryptanalysis

Automatic Search for Key-Bridging Technique: Applications to LBlock and TWINE	247
<i>Li Lin, Wenling Wu, and Yafei Zheng</i>	

MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck	268
<i>Kai Fu, Meiqin Wang, Yinghua Guo, Siwei Sun, and Lei Hu</i>	

Automatic Search for the Best Trails in ARX: Application to Block Cipher SPECK	289
<i>Alex Biryukov, Vesselin Velichkov, and Yann Le Corre</i>	

Designs

Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression	313
<i>Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrede Lepoint, Maria Naya-Plasencia, Pascal Paillier, and Renaud Sirdey</i>	

Efficient Design Strategies Based on the AES Round Function	334
<i>Jérémy Jean and Ivica Nikolić</i>	

Block-Cipher Cryptanalysis

Bit-Based Division Property and Application to SIMON Family	357
<i>Yosuke Todo and Masakatu Morii</i>	

Algebraic Insights into the Secret Feistel Network.	378
<i>Léo Perrin and Aleksei Udovenko</i>	

Integrals Go Statistical: Cryptanalysis of Full Skipjack Variants	399
<i>Meiqin Wang, Tingting Cui, Huaifeng Chen, Ling Sun, Long Wen, and Andrey Bogdanov</i>	

Note on Impossible Differential Attacks.	416
<i>Patrick Derbez</i>	

Improved Linear Hull Attack on Round-Reduced SIMON with Dynamic Key-Guessing Techniques	428
<i>Huaifeng Chen and Xiaoyun Wang</i>	

Foundations and Theory

Modeling Random Oracles Under Unpredictable Queries	453
<i>Pooya Farshim and Arno Mittelbach</i>	
Practical Order-Revealing Encryption with Limited Leakage.	474
<i>Nathan Chenette, Kevin Lewi, Stephen A. Weis, and David J. Wu</i>	
Strengthening the Known-Key Security Notion for Block Ciphers.	494
<i>Benoît Cogliati and Yannick Seurin</i>	
Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications.	514
<i>Peng Wang, Yuling Li, Liting Zhang, and Kaiyan Zheng</i>	

Authenticated-Encryption and Hash Function Cryptanalysis

Key Recovery Attack Against 2.5-Round π -Cipher	535
<i>Christina Boura, Avik Chakraborti, Gaëtan Leurent, Goutam Paul, Dhiman Saha, Hadi Soleimany, and Valentin Suder</i>	
Cryptanalysis of Reduced NORX	554
<i>Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, and Yu Sasaki</i>	
Analysis of the Kupyna-256 Hash Function	575
<i>Christoph Dobraunig, Maria Eichlseder, and Florian Mendel</i>	
Author Index	591

Fast Software Encryption

23rd International Conference, FSE 2016, Bochum,
Germany, March 20-23, 2016, Revised Selected Papers

Peyrin, Th. (Ed.)

2016, XI, 592 p. 105 illus., Softcover

ISBN: 978-3-662-52992-8