

# 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  
*Oscar Reparaz*

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

**Automated Tools for Cryptanalysis**

Automatic Search for Key-Bridging Technique: Applications to LBlock  
 and TWINE . . . . . 247  
*Li Lin, Wenling Wu, and Yafei Zheng*

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

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

**Designs**

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

Efficient Design Strategies Based on the AES Round Function . . . . . 334  
*Jérémy Jean and Ivica Nikolić*

**Block-Cipher Cryptanalysis**

Bit-Based Division Property and Application to SIMON Family . . . . . 357  
*Yosuke Todo and Masakatu Morii*

Algebraic Insights into the Secret Feistel Network. . . . . 378  
*Léo Perrin and Aleksei Udovenko*

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

Note on Impossible Differential Attacks. . . . . 416  
*Patrick Derbez*

Improved Linear Hull Attack on Round-Reduced SIMON with Dynamic  
Key-Guessing Techniques . . . . . 428  
*Huaifeng Chen and Xiaoyun Wang*

**Foundations and Theory**

Modeling Random Oracles Under Unpredictable Queries . . . . . 453  
*Pooya Farshim and Arno Mittelbach*

Practical Order-Revealing Encryption with Limited Leakage. . . . . 474  
*Nathan Chenette, Kevin Lewi, Stephen A. Weis, and David J. Wu*

Strengthening the Known-Key Security Notion for Block Ciphers. . . . . 494  
*Benoît Cogliati and Yannick Seurin*

Related-Key Almost Universal Hash Functions: Definitions,  
Constructions and Applications. . . . . 514  
*Peng Wang, Yuling Li, Liting Zhang, and Kaiyan Zheng*

**Authenticated-Encryption and Hash Function Cryptanalysis**

Key Recovery Attack Against 2.5-Round  $\pi$ -Cipher . . . . . 535  
*Christina Boura, Avik Chakraborti, Gaëtan Leurent, Goutam Paul,  
Dhiman Saha, Hadi Soleimany, and Valentin Suder*

Cryptanalysis of Reduced NORX . . . . . 554  
*Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, and Yu Sasaki*

Analysis of the Kupyna-256 Hash Function . . . . . 575  
*Christoph Dobraunig, Maria Eichlseder, and Florian Mendel*

**Author Index** . . . . . 591



<http://www.springer.com/978-3-662-52992-8>

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