

Contents

Block Cipher Cryptanalysis

Differential Analysis and Meet-in-the-Middle Attack Against Round-Reduced TWINE	3
<i>Alex Biryukov, Patrick Derbez, and Léo Perrin</i>	
Improved Higher-Order Differential Attacks on MISTY1	28
<i>Achiya Bar-On</i>	
Meet-in-the-Middle Technique for Truncated Differential and Its Applications to CLEFIA and Camellia	48
<i>Leibo Li, Keting Jia, Xiaoyun Wang, and Xiaoyang Dong</i>	

Understanding Attacks

Protecting Against Multidimensional Linear and Truncated Differential Cryptanalysis by Decorrelation	73
<i>Céline Blondeau, Ash Bay, and Serge Vaudenay</i>	
Analysis of Impossible, Integral and Zero-Correlation Attacks on Type-II Generalized Feistel Networks Using the Matrix Method.	92
<i>Céline Blondeau and Marine Minier</i>	

Implementation Issues

Simpler and More Efficient Rank Estimation for Side-Channel Security Assessment	117
<i>Cezary Glowacz, Vincent Grosso, Romain Poussier, Joachim Schüth, and François-Xavier Standaert</i>	
Conversion from Arithmetic to Boolean Masking with Logarithmic Complexity	130
<i>Jean-Sébastien Coron, Johann Großschädl, Mehdi Tibouchi, and Praveen Kumar Vadnala</i>	
Comb to Pipeline: Fast Software Encryption Revisited.	150
<i>Andrey Bogdanov, Martin M. Lauridsen, and Elmar Tischhauser</i>	

More Block Cipher Cryptanalysis

Security of the AES with a Secret S-Box	175
<i>Tyge Tiessen, Lars R. Knudsen, Stefan Kölbl, and Martin M. Lauridsen</i>	

Meet-in-the-Middle Attacks and Structural Analysis of Round-Reduced PRINCE	190
<i>Patrick Derbez and Léo Perrin</i>	

Linear Distinguishers in the Key-less Setting: Application to PRESENT	217
<i>Martin M. Lauridsen and Christian Rechberger</i>	

Cryptanalysis of Authenticated Encryption Schemes

Differential-Linear Cryptanalysis of ICEPOLE	243
<i>Tao Huang, Ivan Tjuawinata, and Hongjun Wu</i>	

Cryptanalysis of JAMBU	264
<i>Thomas Peyrin, Siang Meng Sim, Lei Wang, and Guoyan Zhang</i>	

Related-Key Forgeries for Prøst-OTR	282
<i>Christoph Dobraunig, Maria Eichlseder, and Florian Mendel</i>	

Practical Cryptanalysis of the Open Smart Grid Protocol	297
<i>Philipp Jovanovic and Samuel Neves</i>	

Proofs

Relaxing Full-Codebook Security: A Refined Analysis of Key-Length Extension Schemes	319
<i>Peter Gazi, Jooyoung Lee, Yannick Seurin, John Steinberger, and Stefano Tessaro</i>	

The Related-Key Security of Iterated Even–Mansour Ciphers	342
<i>Pooya Farshim and Gordon Procter</i>	

Security of Keyed Sponge Constructions Using a Modular Proof Approach. . . .	364
<i>Elena Andreeva, Joan Daemen, Bart Mennink, and Gilles Van Assche</i>	

GCM Security Bounds Reconsidered	385
<i>Yuichi Niwa, Keisuke Ohashi, Kazuhiko Minematsu, and Tetsu Iwata</i>	

Design

Boosting OMD for Almost Free Authentication of Associated Data.	411
<i>Reza Reyhanitabar, Serge Vaudenay, and Damian Vizár</i>	

Optimally Secure Tweakable Blockciphers	428
<i>Bart Mennink</i>	

Lightweight

On Lightweight Stream Ciphers with Shorter Internal States	451
<i>Frederik Armknecht and Vasily Mikhalev</i>	
Lightweight MDS Involution Matrices	471
<i>Siang Meng Sim, Khoongming Khoo, Frédérique Oggier, and Thomas Peyrin</i>	
A New Classification of 4-bit Optimal S-boxes and Its Application to PRESENT, RECTANGLE and SPONGENT	494
<i>Wentao Zhang, Zhenzhen Bao, Vincent Rijmen, and Meicheng Liu</i>	

Cryptanalysis of Hash Functions and Stream Ciphers

Rotational Cryptanalysis of ARX Revisited	519
<i>Dmitry Khovratovich, Ivica Nikolić, Josef Pieprzyk, Przemysław Sokołowski, and Ron Steinfeld</i>	
Internal Differential Boomerangs: Practical Analysis of the Round-Reduced Keccak- f Permutation	537
<i>Jérémy Jean and Ivica Nikolić</i>	
New Linear Correlations Related to State Information of RC4 PRGA Using IV in WPA	557
<i>Ryoma Ito and Atsuko Miyaji</i>	

Mass Surveillance

A More Cautious Approach to Security Against Mass Surveillance	579
<i>Jean Paul Degabriele, Pooya Farshim, and Bertram Poettering</i>	

Author Index	599
-------------------------------	-----

Fast Software Encryption

22nd International Workshop, FSE 2015, Istanbul,

Turkey, March 8-11, 2015, Revised Selected Papers

Leander, G. (Ed.)

2015, XI, 600 p. 131 illus., Softcover

ISBN: 978-3-662-48115-8