

Table of Contents

Cryptanalysis of Block Ciphers I

The Saturation Attack – A Bait for Twofish	1
<i>Stefan Lucks</i>	
Linear Cryptanalysis of Reduced Round Serpent	16
<i>Eli Biham, Orr Dunkelman, Nathan Keller</i>	
Cryptanalysis of the Mercy Block Cipher	28
<i>Scott R. Fluhrer</i>	

Hash Functions and Boolean Functions

Producing Collisions for PANAMA	37
<i>Vincent Rijmen, Bart Van Rompay, Bart Preneel, Joos Vandewalle</i>	
The RIPEMD ^L and RIPEMD ^R Improved Variants of MD4 Are Not Collision Free	52
<i>Christophe Debaert, Henri Gilbert</i>	
New Constructions of Resilient Boolean Functions with Maximal Nonlinearity	66
<i>Yuriy Tarannikov</i>	

Modes of Operations

Optimized Self-Synchronizing Mode of Operation	78
<i>Ammar Alkassar, Alexander Geraudy, Birgit Pfitzmann, Ahmad-Reza Sadeghi</i>	
Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes	92
<i>Virgil D. Gligor, Pompiliu Donescu</i>	
Incremental Unforgeable Encryption	109
<i>Enrico Buonanno, Jonathan Katz, Moti Yung</i>	

Cryptanalysis of Stream Ciphers I

ZIP Attacks with Reduced Known Plaintext	125
<i>Michael Stay</i>	
Cryptanalysis of the SEAL 3.0 Pseudorandom Function Family	135
<i>Scott R. Fluhrer</i>	

Cryptanalysis of SBLH	144
<i>Goce Jakimovski, Ljupčo Kocarev</i>	

A Practical Attack on Broadcast RC4	152
<i>Itzik Mantin, Adi Shamir</i>	

Cryptanalysis of Block Ciphers II

Improved SQUARE Attacks against Reduced-Round HIEROCRYPT	165
<i>Paulo S.L.M. Barreto, Vincent Rijmen, Jorge Nakahara, Bart Preneel, Joos Vandewalle, Hae Y. Kim</i>	

Differential Cryptanalysis of Q	174
<i>Eli Biham, Vladimir Furman, Michal Misztal, Vincent Rijmen</i>	

Differential Cryptanalysis of Nimbus	187
<i>Vladimir Furman</i>	

Cryptanalysis of Stream Ciphers II

Fast Correlation Attack Algorithm with List Decoding and an Application	196
<i>Miodrag J. Mihaljević, Marc P.C. Fossorier, Hideki Imai</i>	

Bias in the LEVIATHAN Stream Cipher	211
<i>Paul Crowley, Stefan Lucks</i>	

Analysis of SSC2	219
<i>Daniel Bleichenbacher, Willi Meier</i>	

Pseudo-Randomness

Round Security and Super-Pseudorandomness of MISTY Type Structure	233
<i>Tetsu Iwata, Tomonobu Yoshino, Tomohiro Yuasa, Kaoru Kurosawa</i>	

New Results on the Pseudorandomness of Some Blockcipher Constructions	248
<i>Henri Gilbert, Marine Minier</i>	

FSE 2001 Special Talk

NESSIE: A European Approach to Evaluate Cryptographic Algorithms ...	267
<i>Bart Preneel</i>	

Cryptanalysis of Block Ciphers III

Related Key Attacks on Reduced Round KASUMI	277
<i>Mark Blunden, Adrian Escott</i>	

Security of Camellia against Truncated Differential Cryptanalysis	286
<i>Masayuki Kanda, Tsutomu Matsumoto</i>	
Impossible Differential Cryptanalysis of Zodiac	300
<i>Deukjo Hong, Jaechul Sung, Shiho Moriai, Sangjin Lee, Jongin Lim</i>	
Design and Evaluation	
The Block Cipher SC2000	312
<i>Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama,</i> <i>Masahiko Takenaka, Kouichi Itoh, Jun Yajima, Naoya Torii,</i> <i>Hidema Tanaka</i>	
Flaws in Differential Cryptanalysis of Skipjack	328
<i>Louis Granboulan</i>	
Efficient Algorithms for Computing Differential Properties of Addition	336
<i>Helger Lipmaa, Shiho Moriai</i>	
Author Index	351



<http://www.springer.com/978-3-540-43869-4>

Fast Software Encryption

8th International Workshop, FSE 2001 Yokohama,

Japan, April 2-4, 2001, Revised Papers

Matsui, M. (Ed.)

2002, IX, 354 p., Softcover

ISBN: 978-3-540-43869-4