Table of Contents

Cryptanalysis of Block Ciphers I

The Saturation Attack – A Bait for Twofish ......................... 1
  Stefan Lucks

Linear Cryptanalysis of Reduced Round Serpent .................... 16
  Eli Biham, Orr Dunkelman, Nathan Keller

Cryptanalysis of the Mercy Block Cipher ............................ 28
  Scott R. Fluhrer

Hash Functions and Boolean Functions

Producing Collisions for PANAMA .................................... 37
  Vincent Rijmen, Bart Van Rompuy, Bart Preneel, Joos Vandewalle

The RIPEMD\textsuperscript{L} and RIPEMD\textsuperscript{R} Improved Variants of MD4 Are Not Collision Free ..................... 52
  Christophe Debaert, Henri Gilbert

New Constructions of Resilient Boolean Functions with Maximal Nonlinearity ............................................ 66
  Yuriy Tarannikov

Modes of Operations

Optimized Self-Synchronizing Mode of Operation .................... 78
  Ammar Alkassar, Alexander Geraudly, Birgit Pfitzmann,
  Ahmad-Reza Sadeghi

Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes ........................................ 92
  Virgil D. Gligor, Pompiliu Donescu

Incremental Unforgeable Encryption ................................ 109
  Enrico Buonanno, Jonathan Katz, Moti Yung

Cryptanalysis of Stream Ciphers I

ZIP Attacks with Reduced Known Plaintext ........................ 125
  Michael Stay

Cryptanalysis of the SEAL 3.0 Pseudorandom Function Family ....... 135
  Scott R. Fluhrer
VIII Table of Contents

Cryptanalysis of SBLH ......................................................... 144
Goce Jakimovski, Ljupco Kocarev

A Practical Attack on Broadcast RC4 .................................. 152
Itzik Mantin, Adi Shamir

Cryptanalysis of Block Ciphers II

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

Differential Cryptanalysis of Q............................................. 174
Eli Biham, Vladimir Furman, Michal Misztal, Vincent Rijmen

Differential Cryptanalysis of Nimbus .................................... 187
Vladimir Furman

Cryptanalysis of Stream Ciphers II

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

Bias in the LEVIATHAN Stream Cipher .................................. 211
Paul Crowley, Stefan Lucks

Analysis of SSC2 ............................................................ 219
Daniel Bleichenbacher, Willi Meier

Pseudo-Randomness

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

New Results on the Pseudorandomness of Some Blockcipher
Constructions ............................................................. 248
Henri Gilbert, Marine Minier

FSE 2001 Special Talk

NESSIE: A European Approach to Evaluate Cryptographic Algorithms ... 267
Bart Preneel

Cryptanalysis of Block Ciphers III

Related Key Attacks on Reduced Round KASUMI ..................... 277
Mark Blunden, Adrian Escott
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security of Camellia against Truncated Differential Cryptanalysis</td>
<td>286</td>
</tr>
<tr>
<td>Masayuki Kanda, Tsutomu Matsumoto</td>
<td></td>
</tr>
<tr>
<td>Impossible Differential Cryptanalysis of Zodiac</td>
<td>300</td>
</tr>
<tr>
<td>Deukjo Hong, Jaechul Sung, Shiho Moriai, Sangjin Lee, Jongin Lim</td>
<td></td>
</tr>
<tr>
<td>Design and Evaluation</td>
<td></td>
</tr>
<tr>
<td>The Block Cipher SC2000</td>
<td>312</td>
</tr>
<tr>
<td>Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama,</td>
<td></td>
</tr>
<tr>
<td>Masahiko Takenaka, Kowichi Itoh, Jun Yajima, Naoya Torii,</td>
<td></td>
</tr>
<tr>
<td>Hidema Tanaka</td>
<td></td>
</tr>
<tr>
<td>Flaws in Differential Cryptanalysis of Skipjack</td>
<td>328</td>
</tr>
<tr>
<td>Louis Granboulan</td>
<td></td>
</tr>
<tr>
<td>Helger Lipmaa, Shiho Moriai</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>351</td>
</tr>
</tbody>
</table>
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