

Table of Contents

Specific Stream-Cipher Cryptanalysis

Real Time Cryptanalysis of A5/1 on a PC	1
<i>Alex Biryukov, Adi Shamir, and David Wagner</i>	
Statistical Analysis of the Alleged RC4 Keystream Generator	19
<i>Scott R. Fluhrer and David A. McGrew</i>	

New Ciphers

The Software-Oriented Stream Cipher SSC2	31
<i>Muziang Zhang, Christopher Carroll, and Agnes Chan</i>	
Mercy: A Fast Large Block Cipher for Disk Sector Encryption	49
<i>Paul Crowley</i>	

AES Cryptanalysis 1

A Statistical Attack on RC6	64
<i>Henri Gilbert, Helena Handschuh, Antoine Joux, and Serge Vaudenay</i>	
Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent	75
<i>John Kelsey, Tadayoshi Kohno, and Bruce Schneier</i>	
Correlations in RC6 with a Reduced Number of Rounds	94
<i>Lars R. Knudsen and Willi Meier</i>	

Block-Cipher Cryptanalysis 1

On the Interpolation Attacks on Block Ciphers	109
<i>A.M. Youssef and G. Gong</i>	
Stochastic Cryptanalysis of Crypton	121
<i>Marine Minier and Henri Gilbert</i>	

Power Analysis

Bitslice Ciphers and Power Analysis Attacks	134
<i>Joan Daemen, Michael Peeters, and Gilles Van Assche</i>	
Securing the AES Finalists Against Power Analysis Attacks	150
<i>Thomas S. Messerges</i>	

General Stream-Cipher Cryptanalysis

Ciphertext Only Reconstruction of Stream Ciphers based on Combination Generators	165
<i>Anne Canteaut and Eric Filiol</i>	

A Simple Algorithm for Fast Correlation Attacks on Stream Ciphers	181
<i>Vladimor V. Chepyzhov, Thomas Johansson, and Ben Smeets</i>	

A Low-Complexity and High-Performance Algorithm for the Fast Correlation Attack	196
<i>Miodrag J. Mihaljević, Marc P.C. Fossorier, and Hideki Imai</i>	

AES Cryptanalysis 2

Improved Cryptanalysis of Rijndael	213
<i>Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting</i>	

On the Pseudorandomness of the AES Finalists — RC6 and Serpent	231
<i>Tetsu Iwata and Kaoru Kurosawa</i>	

Block-Cipher Cryptanalysis 2

Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Family	244
<i>Jorge Nakahara Jr, Bart Preneel, and Joos Vandewalle</i>	

A Chosen-Plaintext Linear Attack on DES	262
<i>Lars R. Knudsen and John Erik Mathiassen</i>	

Theoretical Work

Provable Security against Differential and Linear Cryptanalysis for the SPN Structure	273
<i>Seokhie Hong, Sangjin Lee, Jongin Lim, Jaechul Sung, Donghyeon Cheon, and Inho Cho</i>	

Unforgeable Encryption and Chosen Ciphertext Secure Modes of Operation	284
<i>Jonathan Katz and Moti Yung</i>	

Efficient Methods for Generating MARS-Like S-Boxes	300
<i>L. Burnett, G. Carter, E. Dawson, and W. Millan</i>	

Author Index	315
--------------------	-----