

# Table of Contents

## Advanced Encryption Standard

Improved Analysis of Some Simplified Variants of RC6.....	1
<i>S. Contini, R.L. Rivest, M.J.B. Robshaw, and Y.L. Yin</i>	
Linear Cryptanalysis of RC5 and RC6.....	16
<i>J. Borst, B. Preneel, and J. Vandewalle</i>	
A Revised Version of CRYPTON: CRYPTON V1.0.....	31
<i>C.H. Lim</i>	
Attack on Six Rounds of CRYPTON.....	46
<i>C. D'Halluin, G. Bijnens, V. Rijmen, and B. Preneel</i>	
On the Security of the 128-bit Block Cipher DEAL.....	60
<i>S. Lucks</i>	
Cryptanalysis of a Reduced Version of the Block Cipher E2.....	71
<i>M. Matsui and T. Tokita</i>	
On the Decorrelated Fast Cipher (DFC) and Its Theory.....	81
<i>L.R. Knudsen and V. Rijmen</i>	

## Remotely Keyed Encryption

Scramble All, Encrypt Small.....	95
<i>M. Jakobsson, J.P. Stern, and M. Yung</i>	
Accelerated Remotely Keyed Encryption.....	112
<i>S. Lucks</i>	

## Analysis of Block Ciphers I

Miss in the Middle Attacks on IDEA and Khufu.....	124
<i>E. Biham, A. Biryukov, and A. Shamir</i>	
Mod $n$ Cryptanalysis, with Applications against RC5P and M6.....	139
<i>J. Kelsey, B. Schneier, and D. Wagner</i>	
The Boomerang Attack.....	156
<i>D. Wagner</i>	

## Miscellaneous

Towards Making Luby-Rackoff Ciphers Optimal and Practical.....	171
<i>S. Patel, Z. Ramzan, and G.S. Sundaram</i>	
A New Characterization of Almost Bent Functions.....	186
<i>A. Canteaut, P. Charpin, and H. Dobbertin</i>	
Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers.....	201
<i>K.G. Paterson</i>	

**Modes of Operation**

On the Security of Double and 2-Key Triple Modes of Operation.....215  
*H. Handschuh and B. Preneel*  
On the Construction of Variable-Input-Length Ciphers ..... 231  
*M. Bellare and P. Rogaway*

**Analysis of Block Ciphers II**

Slide Attacks..... 245  
*A. Biryukov and D. Wagner*  
On the Security of CS-Cipher ..... 260  
*S. Vaudenay*  
Interpolation Attacks of the Block Cipher: SNAKE..... 275  
*S. Moriai, T. Shimoyama, and T. Kaneko*

**Stream Ciphers**

High-Speed Pseudorandom Number Generation with Small Memory ..... 290  
*W. Aiello, S. Rajagopalan, and R. Venkatesan*  
SOBER Cryptanalysis.....305  
*D. Bleichenbacher and S. Patel*

**Author Index** ..... 317

Fast Software Encryption

6th International Workshop, FSE'99 Rome, Italy, March

24-26, 1999 Proceedings

Knudsen, L. (Ed.)

1999, VIII, 324 p., Softcover

ISBN: 978-3-540-66226-6