Contents

1. Cryptanalysis I

χ^2 Cryptanalysis of the SEAL Encryption Algorithm
Helena Handschuh, Henri Gilbert 1

Partitioning Cryptanalysis
Carlo Harpes, James L. Massey 13

The Interpolation Attack on Block Ciphers
Thomas Jakobsen, Lars R. Knudsen 28

Best Differential Characteristic Search of FEAL
Kazumaro Aoki, Kunio Kobayashi, Shiho Moriai 41

2. Blockciphers I

New Block Encryption Algorithm MISTY
Mitsuru Matsui 54

The Design of the ICE Encryption Algorithm
Matthew Kwan 69

3. Discussion

Advanced Encryption Standard, Draft Minimum Requirements and Evaluation Criteria 83

4. Stream Ciphers

TWOPRIME: A Fast Stream Ciphering Algorithm
Cunsheng Ding, Valtteri Niemi, Ari Renvall, Arto Salomaa 88

On Nonlinear Filter Generators
Markus Dichtl 103

Chameleon — A New Kind of Stream Cipher
Ross Anderson, Charalampos Manifavas 107

5. Cryptanalysis II

Improving Linear Cryptanalysis of LOKI91 by Probabilistic Counting Method
Kouichi Sakurai, Souichi Furuya 114

Cryptanalysis of Ladder-DES
Eli Biham 134

A Family of Trapdoor Ciphers
Vincent Rijmen, Bart Preneel 139

6. Blockciphers II

The Block Cipher Square
Joan Daemen, Lars Knudsen, Vincent Rijmen 149

xmx - A Firmware-Oriented Block Cipher Based on Modular Multiplications
David M'Raïhi, David Naccache, Jacques Stern, Serge Vaudenay 166

7. Message Authentication Codes

MMH: Software Message Authentication in the Gbit/Second Rates
Shai Halevi, Hugo Krawczyk 172

Fast Message Authentication Using Efficient Polynomial Evaluation
Valentine Afanassiev, Christian Gehrmann, Ben Smeets 190

Reinventing the Travois: Encryption/MAC in 30 ROM Bytes
Gideon Yuval 205

8. Modes of Operation

All-or-Nothing Encryption and the Package Transform
Ronald L. Rivest 210

On the Security of Remotely Keyed Encryption
Stefan Lucks 219

Sliding Encryption: A Cryptographic Tool for Mobile Agents
Adam Young, Moti Yung 230

9. Fast Software Encryption

Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor
Bruce Schneier, Doug Whiting 242

A Fast New DES Implementation in Software
Eli Biham 260

Optimizing a Fast Stream Cipher for VLIW, SIMD, and Superscalar Processors
Craig S.K. Clapp 273

Author Index 289