

Table of Contents

Cryptanalysis I

New Results in Linear Cryptanalysis of RC5.....	1
<i>Ali Aydın Selçuk (University of Maryland Baltimore County)</i>	
Higher Order Differential Attack of a CAST Cipher	17
<i>Shiho Moriai, Takeshi Shimoyama (TAO), Toshinobu Kaneko (TAO, Science University of Tokyo)</i>	
Cryptanalysis of TWOPRIME	32
<i>Don Coppersmith (IBM Research), David Wagner (U.C. Berkeley), Bruce Schneier, John Kelsey (Counterpane Systems)</i>	

New Stream Ciphers

JEROBOAM	49
<i>Hervé Chabanne (SAGEM SA), Emmanuel Michon (Ecole Polytechnique)</i>	
Fast Hashing and Stream Encryption with PANAMA	60
<i>Joan Daemen (Banksys), Craig S.K. Clapp (PictureTel Corporation)</i>	
Joint Hardware / Software Design of a Fast Stream Cipher	75
<i>Craig S.K. Clapp (PictureTel Corporation)</i>	

Design Construction Analysis

On the Security of the Hashing Scheme Based on SL_2	93
<i>Kanat S. Abdukhalikov (Institute for Pure and Applied Mathematics, Kazakhstan), Chul Kim (Kwangwoon University)</i>	
About Feistel Schemes with Six (or more) Rounds.....	103
<i>Jacques Patarin (BULL PTS)</i>	
Monkey: Black-Box Symmetric Ciphers Designed for MONopolizingKEYs .	122
<i>Adam Young (Columbia University), Moti Yung (CertCo)</i>	

Hash Functions

MRD Hashing	134
<i>Rei Safavi-Naini, Shahram Bakhtiari, Chris Charnes (University of Wollongong)</i>	

New Constructions for Secure Hash Functions	150
<i>William Aiello (BellCore), Stuart Haber (Surety), Ramarathnam Venkatesan (Microsoft Research)</i>	

Pseudo-Random Generators

Cryptanalytic Attacks on Pseudorandom Number Generators	168
<i>John Kelsey, Bruce Schneier (Counterpane Systems), David Wagner (University of California Berkeley), Chris Hall (Counterpane Systems)</i>	

New Block Ciphers

CS-CIPHER	189
<i>Jacques Stern, Serge Vaudenay (Ecole Normale Supérieure)</i>	
On the Design and Security of RC2	206
<i>Lars R. Knudsen (University of Bergen), Vincent Rijmen (K.U. Leuven), Ronald L. Rivest (MIT), Matthew J.B. Robshaw (RSA Laboratories)</i>	
Serpent: A New Block Cipher Proposal	222
<i>Eli Biham (Technion), Ross Anderson (Cambridge University), Lars R. Knudsen (University of Bergen)</i>	

Modes of Operations

Attacking Triple Encryption	239
<i>Stefan Lucks (University of Mannheim)</i>	
Cryptanalysis of some Recently-Proposed Multiple Modes of Operation ...	254
<i>David Wagner (University of California, Berkeley)</i>	

Cryptanalysis II

Differential Cryptanalysis of the ICE Encryption Algorithm	270
<i>Bart Van Rompay (K.U. Leuven), Lars R. Knudsen (University of Bergen), Vincent Rijmen (K.U. Leuven)</i>	
The First Two Rounds of MD4 are Not One-Way	284
<i>Hans Dobbertin (German Information Security Agency)</i>	
Differential Cryptanalysis of KHF	293
<i>David Wagner (University of California, Berkeley)</i>	
Author Index	297