

Table of Contents

Block Cipher Cryptanalysis

Cryptanalysis of IDEA-X/2	1
<i>Håvard Raddum (University of Bergen)</i>	
Differential-Linear Cryptanalysis of Serpent	9
<i>Eli Biham, Orr Dunkelman, and Nathan Keller (Technion)</i>	
Rectangle Attacks on 49-Round SHACAL-1	22
<i>Eli Biham, Orr Dunkelman, and Nathan Keller (Technion)</i>	
Cryptanalysis of Block Ciphers Based on SHA-1 and MD5	36
<i>Markku-Juhani O. Saarinen (Helsinki University of Technology)</i>	
Analysis of Involutional Ciphers: Khazad and Anubis	45
<i>Alex Biryukov (Katholieke Universiteit Leuven)</i>	

Boolean Functions and S-Boxes

On Plateaued Functions and Their Constructions	54
<i>Claude Carlet and Emmanuel Prouff (INRIA)</i>	
Linear Redundancy in S-Boxes	74
<i>Joanne Fuller and William Millan (Queensland University of Technology)</i>	

Stream Cipher Cryptanalysis

Loosening the KNOT	87
<i>Antoine Joux and Frédéric Muller (DCSSI Crypto Lab)</i>	
On the Resynchronization Attack	100
<i>Jovan Dj. Golić (Telecom Italia Lab) and Guglielmo Morgari (Telsy Elettronica e Telecomunicazioni)</i>	
Cryptanalysis of SOBER-t32	111
<i>Steve Babbage (Vodafone Group Research & Development), Christophe De Cannière, Joseph Lano, Bart Preneel, and Joos Vandewalle (Katholieke Universiteit Leuven)</i>	

MACs

OMAC: One-Key CBC MAC	129
<i>Tetsu Iwata and Kaoru Kurosawa (Ibaraki University)</i>	

A Concrete Security Analysis for 3GPP-MAC 154
*Dowon Hong, Ju-Sung Kang (ETRI), Bart Preneel (Katholieke
Universiteit Leuven), and Heuisu Ryu (ETRI)*

New Attacks against Standardized MACs 170
*Antoine Joux, Guillaume Poupard (DCSSI),
and Jacques Stern (Ecole normale supérieure)*

Analysis of RMAC 182
*Lars R. Knudsen (Technical University of Denmark)
and Tadayoshi Kohno (UCSD)*

Side Channel Attacks

A Generic Protection against High-Order Differential Power Analysis 192
*Mehdi-Laurent Akkar and Louis Goubin
(Schlumberger Smart Cards)*

A New Class of Collision Attacks and Its Application to DES 206
*Kai Schramm, Thomas Wollinger, and Christof Paar
(Ruhr-Universität Bochum)*

Block Cipher Theory

Further Observations on the Structure of the AES Algorithm 223
Beomsik Song and Jennifer Seberry (University of Wollongong)

Optimal Key Ranking Procedures in a Statistical Cryptanalysis 235
*Pascal Junod and Serge Vaudenay
(Swiss Federal Institute of Technology, Lausanne)*

Improving the Upper Bound on the Maximum Differential
and the Maximum Linear Hull Probability for SPN Structures and AES .. 247
*Sangwoo Park (National Security Research Institute), Soo Hak Sung
(Pai Chai University), Sangjin Lee, and Jongin Lim (CIST)*

Linear Approximations of Addition Modulo 2^n 261
Johan Wallén (Helsinki University of Technology)

Block Ciphers and Systems of Quadratic Equations 274
*Alex Biryukov and Christophe De Cannière
(Katholieke Universiteit Leuven)*

New Designs

Turing: A Fast Stream Cipher 290
Gregory G. Rose and Philip Hawkes (Qualcomm Australia)

Rabbit: A New High-Performance Stream Cipher	307
<i>Martin Boesgaard, Mette Vesterager, Thomas Pedersen, Jesper Christiansen, and Ove Scavenius (CRYPTICO)</i>	
Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive	330
<i>Niels Ferguson (MacFergus), Doug Whiting (HiFn), Bruce Schneier (Counterpane Internet Security), John Kelsey, Stefan Lucks (Universität Mannheim), and Tadayoshi Kohno (UCSD)</i>	
PARSHA-256 – A New Parallelizable Hash Function and a Multithreaded Implementation	347
<i>Pinakpani Pal and Palash Sarkar (Indian Statistical Institute)</i>	
Modes of Operation	
Practical Symmetric On-Line Encryption	362
<i>Pierre-Alain Fouque, Gwenaëlle Martinet, and Guillaume Poupard (DCSSI Crypto Lab)</i>	
The Security of “One-Block-to-Many” Modes of Operation	376
<i>Henri Gilbert (France Télécom)</i>	
Author Index	397