

# Lecture Notes in Computer Science

2887

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Thomas Johansson (Ed.)

# Fast Software Encryption

10th International Workshop, FSE 2003  
Lund, Sweden, February 24-26, 2003  
Revised Papers



Springer

## Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

## Volume Editor

Thomas Johansson  
Lund University, Department of Information Technology  
Box 118, SE-221 00 Lund, Sweden  
E-mail: thomas@it.lth.se

## Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek  
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;  
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): E.3, F.2.1, E.4, G.4

ISSN 0302-9743

ISBN 3-540-20449-0 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springeronline.com>

© International Association for Cryptologic Research 2003  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP Berlin GmbH  
Printed on acid-free paper      SPIN: 10966228      06/3142      5 4 3 2 1 0

# Preface

Fast Software Encryption is now a 10-year-old workshop on symmetric cryptography, including the design and cryptanalysis of block and stream ciphers, as well as hash functions. The first FSE workshop was held in Cambridge in 1993, followed by Leuven in 1994, Cambridge in 1996, Haifa in 1997, Paris in 1998, Rome in 1999, New York in 2000, Yokohama in 2001, and Leuven in 2002.

This Fast Software Encryption workshop, FSE 2003, was held February 24–26, 2003 in Lund, Sweden. The workshop was sponsored by IACR (International Association for Cryptologic Research) and organized by the General Chair, Ben Smeets, in cooperation with the Department of Information Technology, Lund University.

This year a total of 71 papers were submitted to FSE 2003. After a two-month reviewing process, 27 papers were accepted for presentation at the workshop. In addition, we were fortunate to have in the program an invited talk by James L. Massey.

The selection of papers was difficult and challenging work. Each submission was refereed by at least three reviewers. I would like to thank the program committee members, who all did an excellent job. In addition, I gratefully acknowledge the help of a number of colleagues who provided reviews for the program committee. They are: Kazumaro Aoki, Alex Biryukov, Christophe De Cannière, Nicolas Courtois, Jean-Charles Faugère, Rob Johnson, Pascal Junod, Joseph Lano, Marine Minier, Elisabeth Oswald, Håvard Raddum, and Markku-Juhani O. Saarinen.

The local arrangements for the workshop were managed by a committee consisting of Patrik Ekdahl, Lena Månsson and Laila Lembke. I would like to thank them all for their hard work. Finally, we are grateful for the financial support for the workshop provided by Business Security, Ericsson Mobile Platforms, and RSA Security.

August 2003

Thomas Johansson

# FSE 2003

February 24–26, 2003, Lund, Sweden

Sponsored by the  
*International Association for Cryptologic Research*

in cooperation with  
*Department of Information Technology, Lund University, Sweden*

**Program Chair**  
Thomas Johansson (Lund University, Sweden)

**General Chair**  
Ben Smeets (Ericsson, Sweden)

## Program Committee

Ross Anderson	Cambridge University, UK
Anne Canteaut	Inria, France
Joan Daemen	Protonworld, Belgium
Cunsheng Ding	Hong Kong University of Science and Technology
Hans Dobbertin	University of Bochum, Germany
Henri Gilbert	France Telecom, France
Jovan Golic	Gemplus, Italy
Lars Knudsen	Technical University of Denmark
Helger Lipmaa	Helsinki University of Technology, Finland
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	Fachhochschule Aargau, Switzerland
Kaisa Nyberg	Nokia, Finland
Bart Preneel	K.U. Leuven, Belgium
Vincent Rijmen	Cryptomathic, Belgium
Matt Robshaw	Royal Holloway, University of London, UK
Serge Vaudenay	EPFL, Switzerland
David Wagner	U.C. Berkeley, USA

# 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</i> <i>(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)</i> <i>and Guglielmo Morgari (Telsy Elettronica e Telecomunicazioni)</i>	
Cryptanalysis of SOBER-t32 .....	111
<i>Steve Babbage (Vodafone Group Research &amp; Development),</i> <i>Christophe De Cannière, Joseph Lano, Bart Preneel,</i> <i>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>	
<b>Modes of Operation</b>	
Practical Symmetric On-Line Encryption .....	362
<i>Pierre-Alain Fouque, Gwenaelle 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>	
<b>Author Index</b> .....	397