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

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

http://www.springeronline.com

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

Boolean Functions and S-Boxes

Stream Cipher Cryptanalysis

MACs

Side Channel Attacks

Block Cipher Theory

New Designs

Modes of Operation