Lecture Notes in Computer Science 2365

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

Springer
*Berlin*
*Heidelberg*
*New York*
*Barcelona*
*Hong Kong*
*London*
*Milan*
*Paris*
*Tokyo*

Joan Daemen Vincent Rijmen (Eds.)

# Fast Software Encryption

9th International Workshop, FSE 2002
Leuven, Belgium, February 4-6, 2002
Revised Papers

Springer

Series Editors

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

Volume Editors

Joan Daemen
Proton World
Zweefvliegtuigstraat 10
1130 Brussel, Belgium
E-mail: joan.daemen@protonworld.com

Vincent Rijmen
Cryptomathic
Lei 8A
3000 Leuven, Belgium
E-mail: vincent.rijmen@cryptomathic.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fast software encryption : 9th international workshop ; revised papers / FSE 2002, Leuven, Belgium, February 2002. Joan Daemen ; Vincent Rijmen (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2365)
ISBN 3-540-44009-7

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

ISSN 0302-9743
ISBN 3-540-44009-7 Springer-Verlag Berlin Heidelberg New York



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

http://www.springer.de


Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna e.K.
Printed on acid-free paper SPIN: 10870318 06/3142 5 4 3 2 1 0

# Preface

This Fast Software Encryption workshop was the ninth in a series of workshops started in Cambridge in December 1993. The previous workshop took place in Yokohama in April 2001. It concentrated on all aspects of fast primitives for symmetric cryptography: secret key ciphers, the design and cryptanalysis of block and stream ciphers, as well as hash functions and message authentication codes (MACs).

The ninth Fast Software Encryption workshop was held in February 2002 in Leuven, Belgium and was organized by General Chair Matt Landrock (Cryptomathic Belgium), in cooperation with the research group COSIC of K.U. Leuven. This year there were 70 submissions, of which 21 were selected for presentation and publication in this volume.

We would like to thank the following people. First of all the submitting authors and the program committee for their work. Then Markku-Juhani O. Saarinen, Orr Dunkelman, Fredrik Jönsson, Helger Lipmaa, Greg Rose, Alex Biryukov, and Christophe De Canniere, who provided reviews at the request of program committee members. Bart Preneel for letting us use COSIC's Web-review software in the review process and Wim Moreau for all his support. Finally we would like to thank Krista Geens of Cryptomathic for her help in the registration and the practical organization.

May 2002 Joan Daemen and Vincent Rijmen

# Fast Software Encryption 2002

February 4–6, 2002, Leuven, Belgium

Sponsored by the
*International Association for Cryptologic Research*

### General Chair

Matt Landrock, Cryptomathic, Belgium

### Program Co-chairs

Joan Daemen, Proton World, Belgium
Vincent Rijmen, Cryptomathic, Belgium

### Program Committee

Ross Anderson ..... Cambridge University, UK
Eli Biham ..... Technion, IL
Don Coppersmith ..... IBM, USA
Cunshen Ding ..... Hong Kong University of Science and Technology, HK
Thomas Johansson ..... Lund University, SE
Mitsuru Matsui ..... Mitsubishi Electric, JP
Willi Meier ..... Fachhochschule Aargau, CH
Kaisa Nyberg ..... Nokia, FI
Bart Preneel ..... Katholieke Universiteit Leuven, BE

# Table of Contents

## Block Cipher Cryptanalysis



## Integral Cryptanalysis

## Block Cipher Theory



## Stream Cipher Design



## Stream Cipher Cryptanalysis



## Odds and Ends