Lecture Notes in Computer Science 1008
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Bart Preneel (Ed.)

Fast Software Encryption

Second International Workshop
Leuven, Belgium, December 14-16, 1994
Proceedings

Springer

Series Editors

Gerhard Goos
Universität Karlsruhe
Vincenz-Priessnitz-Straße 3, D-76128 Karlsruhe, Germany

Juris Hartmanis
Department of Computer Science, Cornell University
4130 Upson Hall, Ithaca, NY 14853, USA

Jan van Leeuwen
Department of Computer Science,Utrecht University
Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editor

Bart Preneel
Department Elektrotechniek-ESAT, Katholieke Universiteit Leuven
Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fast software encryption : second international workshop, Leuven, Belgium, December 14 - 16, 1994 ; proceedings / Bart Preneel (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 1995
(Lecture notes in computer science ; Vol. 1008)
ISBN 3-540-60590-8
NE: Preneel, Bart [Hrsg.]; GT

CR Subject Classification (1991): E.3, F2.1, E.4, G.2.1, G.4

ISBN 3-540-60590-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10487173 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

CONTENTS

Session 3: Stream Ciphers–Cryptanalysis

Chair: Cunsheng Ding

Session 4: Block Ciphers—Differential Cryptanalysis

Chair: Eli Biham

Session 5: Block Ciphers–Linear Cryptanalysis

Chair: Bart Preneel

Fast Software Encryption

Katholieke Universiteit Leuven

Leuven, Belgium, December 14–16, 1994

Organizing committee:

Bart Preneel (ESAT, Katholieke Universiteit Leuven) – Chair
Ross Anderson (University Computer Laboratory, Cambridge)
Eli Biham (Technion, Haifa)
Cunsheng Ding (University of Turku, Finland)
Dieter Gollmann (Royal Holloway College, University of London)
James Massey (Swiss Federal Institute of Technology, Zürich)

In cooperation with:

The International Association for Cryptologic Research (IACR)

Sponsored by:

Europay International
Microsoft