

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

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 1995

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10487173 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

CONTENTS

<i>Introduction</i>	1
Bart Preneel	

Session 1: Stream Ciphers—Design

Chair: Dieter Gollmann

<i>Clock-controlled pseudorandom generators on finite groups</i>	6
Ulrich Baum and Simon Blackburn	
<i>On random mappings and random permutations</i>	22
William G. Chambers	
<i>Binary cyclotomic generators</i>	29
Cunsheng Ding	
<i>Construction of bent functions and balanced Boolean functions with high nonlinearity</i>	61
Hans Dobbertin	
<i>Additive and linear structures of cryptographic functions</i>	75
Xuejia Lai	

Session 2: Block Ciphers—Design

Chair: James Massey

<i>The RC5 encryption algorithm</i>	86
Ronald L. Rivest	
<i>The MacGuffin block cipher algorithm</i>	97
Matthew Blaze and Bruce Schneier	
<i>S-boxes and round functions with controllable linearity and differential uniformity</i>	111
Kaisa Nyberg	
<i>Properties of linear approximation tables</i>	131
Luke O'Connor	

Session 3: Stream Ciphers—Cryptanalysis

Chair: Cunsheng Ding

<i>Searching for the optimum correlation attack</i>	137
Ross Anderson	
<i>A known plaintext attack on the PKZIP stream cipher</i>	144
Eli Biham and Paul C. Kocher	
<i>Linear cryptanalysis of stream ciphers</i>	154
Jovan Dj. Golić	
<i>Feedback with carry shift registers over finite fields</i>	170
Andrew Klapper	
<i>A free energy minimization framework for inference problems in modulo 2 arithmetic</i>	179
David J.C. MacKay	

Session 4: Block Ciphers—Differential Cryptanalysis

Chair: Eli Biham

<i>Truncated and higher order differentials</i>	196
Lars R. Knudsen	
<i>SAFER K-64: One year later</i>	212
James L. Massey	
<i>Improved characteristics for differential cryptanalysis of hash functions based on block ciphers</i>	242
Vincent Rijmen and Bart Preneel	

Session 5: Block Ciphers—Linear Cryptanalysis

Chair: Bart Preneel

<i>Linear cryptanalysis using multiple approximations and FEAL</i>	249
Burton S. Kaliski Jr. and Matt J.B. Robshaw	
<i>Problems with the linear cryptanalysis of DES using more than one active S-box per round</i>	265
Uwe Blöcher and Markus Dichtl	

<i>Correlation matrices</i>	275
Joan Daemen, René Govaerts, and Joos Vandewalle	

Session 6: Odds and Ends

Chair: Ross Anderson

<i>On the need for multipermutations: Cryptanalysis of MD4 and SAFER</i> ..	286
Serge Vaudenay	
<i>How to exploit the intractability of exact TSP for cryptography</i>	298
Stefan Lucks	

Session 7: New Algorithms and Protocols

Chair: Eli Biham

<i>How to reverse engineer an EES device</i>	305
Michael Roe	
<i>A fast homophonic coding algorithm based on arithmetic coding</i>	329
Walter T. Penzhorn	

Session 8: Recent Results

Chair: Bart Preneel

<i>On Fibonacci keystream generators</i>	346
Ross Anderson	
<i>Cryptanalysis of McGuffin</i>	353
Vincent Rijmen and Bart Preneel	
<i>Performance of block ciphers and hash functions — one year later</i>	359
Michael Roe	
<i>TEA, a tiny encryption algorithm</i>	363
David J. Wheeler and Roger M. Needham	

Author Index	367
---------------------------	-----

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