

Lecture Notes in Computer Science

1267

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

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

Springer

Berlin

Heidelberg

New York

Barcelona

Budapest

Hong Kong

London

Milan

Paris

Santa Clara

Singapore

Tokyo

Eli Biham (Ed.)

Fast Software Encryption

4th International Workshop, FSE'97
Haifa, Israel, January 20-22, 1997
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Eli Biham

Technion — Israel Institute of Technology, Computer Science Department

Haifa 32000, Israel

E-mail: biham@cs.technion.ac.il

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Fast software encryption : 4th international workshop ;
proceedings / FSE '97, Haifa, Israel, January 20 - 22, 1997. Eli
Biham (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest
; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ;
Tokyo : Springer, 1997
(Lecture notes in computer science ; Vol. 1267)
ISBN 3-540-63247-6**

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

ISSN 0302-9743

ISBN 3-540-63247-6 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 1997

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10548880 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This fast software encryption workshop (FSE) follows the previous three workshops held in Cambridge in December 1993, in Leuven in December 1994, and in Cambridge in February 1996. The workshop was organized in cooperation with the International Association for Cryptologic Research (IACR), and with the kind support of Algorithmic Research and of Microsoft. It was held at the Technion (Haifa, Israel), January 20–22, 1997. The programme committee consisted of Eli Biham (Technion - chair), Ross Anderson (Cambridge University), Don Coppersmith (IBM Research), Cunsheng Ding (Turku), Dieter Gollmann (Royal Holloway), Jim Massey (ETH Zurich), Mitsuru Matsui (Mitsubishi), and Bart Preneel (Katholieke Universiteit Leuven). Next year's fast software encryption workshop will be organized by Serge Vaudenay and will be held in Paris.

This series of workshops concentrates on the theory and practice of fast cryptography, and in particular of blockciphers, stream ciphers, hash functions, and message authentication codes. The presentations deal with new suggestions of such cryptographic primitives, their design, and their analysis. Special preference is given to the applicability of these primitives in software, and their fast implementations. On the other hand, applications and analyses of other cryptographic primitives, and in particular of public key cryptosystems, are beyond the scope of the workshops, and their design and analysis is dealt with in other conferences and workshops on cryptography.

This year, 44 papers were submitted to the workshop. Each of these papers was refereed by at least three programme committee members. All the reports were later sent to the respective authors. Based on the reports, 23 papers were selected for presentation at the workshop, including seven papers on cryptanalysis, four papers suggesting new blockciphers, three dealing with stream ciphers, three with message authentication codes, three with modes of operation, and three papers with the core of fast software encryption, i.e., how to design fast encryption in software.

In addition, two discussion sessions were held: a discussion on the requirements and evaluation criteria for the Advanced Encryption Standard, whose development process was recently announced by the US National Institute of Standards and Technology (NIST), and a discussion on the security of cryptosystems and the relation between theory and practice. The minutes of the first discussion are included in these proceedings.

The workshop was organized almost entirely using email and WWW. A home page was created for the workshop, through which all the information on the workshop was distributed: the call for papers, registration and general information, acceptance of papers, and the workshop's program. All the papers were submitted using email (except for two papers submitted in paper form), and

all the distribution of papers to the programme committee and the discussions of the programme committee were done using email. In addition, all the papers were processed directly from their \LaTeX files, using the llncs style, and were automatically merged into these proceedings.

These proceedings follow the tradition of this series of workshops whose proceedings have been published in Springer-Verlag's Lecture Notes in Computer Science (LNCS) series: The proceedings of the first FSE workshop, held in Cambridge in 1993, were published as LNCS 809, the proceedings of the second FSE workshop, held in Leuven in 1994, were published as LNCS 1008, and the proceedings of the third FSE workshop, held in Cambridge in 1996, were published as LNCS 1039.

I would like to thank the authors for their submissions and the participants for attending the workshop. The programme committee deserves special thanks for their hard work. Simon Blackburn, Antoon Bosselaers, Karl Brincat, Mike Burmester, Lars Knudsen, Sean Murphy, Kenneth G. Paterson, Vincent Rijmen, Serge Vaudenay, and Peter Wild are acknowledged for their services as external referees. It is also a pleasure to thank the Department of External Studies of the Technion, and in particular Pnina Sasson, who made all the local arrangements, and to thank Yvonne Sagi for her help in preparing some of the material for the workshop. Finally, special thanks go to the sponsors for their generous support.

May 1997

Eli Biham

Contents

1. Cryptanalysis I

<i>χ^2 Cryptanalysis of the SEAL Encryption Algorithm</i> Helena Handschuh, Henri Gilbert	1
<i>Partitioning Cryptanalysis</i> Carlo Harpes, James L. Massey	13
<i>The Interpolation Attack on Block Ciphers</i> Thomas Jakobsen, Lars R. Knudsen	28
<i>Best Differential Characteristic Search of FEAL</i> Kazumaro Aoki, Kunio Kobayashi, Shiho Moriai	41

2. Blockciphers I

<i>New Block Encryption Algorithm MISTY</i> Mitsuru Matsui	54
<i>The Design of the ICE Encryption Algorithm</i> Matthew Kwan	69

3. Discussion

<i>Advanced Encryption Standard, Draft Minimum Requirements and Evaluation Criteria</i>	83
---	----

4. Stream Ciphers

<i>TWOPRIME: A Fast Stream Ciphering Algorithm</i> Cunsheng Ding, Valteri Niemi, Ari Renvall, Arto Salomaa	88
<i>On Nonlinear Filter Generators</i> Markus Dichtl	103
<i>Chameleon — A New Kind of Stream Cipher</i> Ross Anderson, Charalampos Maniavas	107

5. Cryptanalysis II

<i>Improving Linear Cryptanalysis of LOKI91 by Probabilistic Counting Method</i> Kouichi Sakurai, Souichi Furuya	114
<i>Cryptanalysis of Ladder-DES</i> Eli Biham	134
<i>A Family of Trapdoor Ciphers</i> Vincent Rijmen, Bart Preneel	139

6. Blockciphers II

The Block Cipher Square

Joan Daemen, Lars Knudsen, Vincent Rijmen 149

xmx - A Firmware-Oriented Block Cipher Based on Modular Multiplications

David M'Raihi, David Naccache, Jacques Stern, Serge Vaudenay 166

7. Message Authentication Codes

MMH: Software Message Authentication in the Gbit/Second Rates

Shai Halevi, Hugo Krawczyk 172

Fast Message Authentication Using Efficient Polynomial Evaluation

Valentine Afanassiev, Christian Gehrman, Ben Smeets 190

Reinventing the Travois: Encryption/MAC in 30 ROM Bytes

Gideon Yuval 205

8. Modes of Operation

All-or-Nothing Encryption and the Package Transform

Ronald L. Rivest 210

On the Security of Remotely Keyed Encryption

Stefan Lucks 219

Sliding Encryption: A Cryptographic Tool for Mobile Agents

Adam Young, Moti Yung 230

9. Fast Software Encryption

Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor

Bruce Schneier, Doug Whiting 242

A Fast New DES Implementation in Software

Eli Biham 260

Optimizing a Fast Stream Cipher for VLIW, SIMD, and Superscalar Processors

Craig S.K. Clapp 273

Author Index 289