

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

1978

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Bruce Schneier (Ed.)

Fast Software Encryption

7th International Workshop, FSE 2000
New York, NY, USA, April 10-12, 2000
Proceedings



Springer

Series Editors

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

Volume Editor

Bruce Schneier
Counterpane Internet Security, Inc.
3031 Tisch Way, Suite 100PE, San Jose, CA 95128, USA
E-mail: schneier@counterpane.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fast software encryption : 7th international workshop ; proceedings /
FSE 2000, New York, NY, April 10 - 12, 2000. Bruce Schneider (ed.). -
Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 1978)
ISBN 3-540-41728-1

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

ISSN 0302-9743

ISBN 3-540-41728-1 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 New York
a member of BertelsmannSpringer Science+Business Media GmbH
© Springer-Verlag Berlin Heidelberg 2001
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP Berlin, Stefan Sossna
Printed on acid-free paper SPIN 10781399 06/3142 5 4 3 2 1 0

Preface

Since 1993, cryptographic algorithm research has centered around the Fast Software Encryption (FSE) workshop. First held at Cambridge University with 30 attendees, it has grown over the years and has achieved worldwide recognition as a premiere conference. It has been held in Belgium, Israel, France, Italy, and, most recently, New York.

FSE 2000 was the 7th international workshop, held in the United States for the first time. Two hundred attendees gathered at the Hilton New York on Sixth Avenue, to hear 21 papers presented over the course of three days: 10–12 April 2000. These proceedings constitute a collection of the papers presented during those days.

FSE concerns itself with research on classical encryption algorithms and related primitives, such as hash functions. This branch of cryptography has never been more in the public eye. Since 1997, NIST has been shepherding the Advanced Encryption Standard (AES) process, trying to select a replacement algorithm for DES. The first AES conference, held in California the week before Crypto 98, had over 250 attendees. The second conference, held in Rome two days before FSE 99, had just under 200 attendees. The third AES conference was held in conjunction with FSE 2000, during the two days following it, at the same hotel.

It was a great pleasure for me to organize and chair FSE 2000. We received 53 submissions covering the broad spectrum of classical encryption research. Each of those submissions was read by at least three committee members – more in some cases. The committee chose 21 papers to be presented at the workshop. Those papers were distributed to workshop attendees in a preproceedings volume. After the workshop, authors were encouraged to further improve their papers based on comments received. The final result is the proceedings volume you hold in your hand.

To conclude, I would like to thank all the authors who submitted papers to this conference, whether or not your papers were accepted. It is your continued research that makes this field a vibrant and interesting one. I would like to thank the other program committee members: Ross Anderson (Cambridge), Eli Biham (Technion), Don Coppersmith (IBM), Cunsheng Ding (Singapore), Dieter Gollmann (Microsoft), Lars Knudsen (Bergen), James Massey (Lund), Mitsuru Matsui (Mitsubishi), Bart Preneel (K.U.Leuven), and Serge Vaudenay (EPFL). They performed the hard – and too often thankless – task of selecting the program. I'd like to thank my assistant, Beth Friedman, who handled administrative matters for the conference. And I would like to thank the attendees for coming to listen, learn, share ideas, and participate in the community. I believe that FSE represents the most interesting subgenre within cryptography, and that this conference represents the best of what cryptography has to offer.

Enjoy the proceedings, and I'll see everyone next year in Japan.

Table of Contents

Specific Stream-Cipher Cryptanalysis

Real Time Cryptanalysis of A5/1 on a PC 1
Alex Biryukov, Adi Shamir, and David Wagner

Statistical Analysis of the Alleged RC4 Keystream Generator 19
Scott R. Fluhrer and David A. McGrew

New Ciphers

The Software-Oriented Stream Cipher SSC2 31
Muxiang Zhang, Christopher Carroll, and Agnes Chan

Mercy: A Fast Large Block Cipher for Disk Sector Encryption 49
Paul Crowley

AES Cryptanalysis 1

A Statistical Attack on RC6 64
Henri Gilbert, Helena Handschuh, Antoine Joux, and Serge Vaudenay

Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent 75
John Kelsey, Tadayoshi Kohno, and Bruce Schneier

Correlations in RC6 with a Reduced Number of Rounds 94
Lars R. Knudsen and Willi Meier

Block-Cipher Cryptanalysis 1

On the Interpolation Attacks on Block Ciphers 109
A.M. Youssef and G. Gong

Stochastic Cryptanalysis of Crypton 121
Marine Minier and Henri Gilbert

Power Analysis

Bitslice Ciphers and Power Analysis Attacks 134
Joan Daemen, Michael Peeters, and Gilles Van Assche

Securing the AES Finalists Against Power Analysis Attacks 150
Thomas S. Messerges

General Stream-Cipher Cryptanalysis

Ciphertext Only Reconstruction of Stream Ciphers based on Combination Generators	165
<i>Anne Canteaut and Eric Filiol</i>	

A Simple Algorithm for Fast Correlation Attacks on Stream Ciphers	181
<i>Vladimir V. Chepyzhov, Thomas Johansson, and Ben Smeets</i>	

A Low-Complexity and High-Performance Algorithm for the Fast Correlation Attack	196
<i>Miodrag J. Mihajević, Marc P.C. Fossorier, and Hideki Imai</i>	

AES Cryptanalysis 2

Improved Cryptanalysis of Rijndael	213
<i>Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting</i>	

On the Pseudorandomness of the AES Finalists — RC6 and Serpent	231
<i>Tetsu Iwata and Kaoru Kurosawa</i>	

Block-Cipher Cryptanalysis 2

Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Family	244
<i>Jorge Nakahara Jr, Bart Preneel, and Joos Vandewalle</i>	

A Chosen-Plaintext Linear Attack on DES	262
<i>Lars R. Knudsen and John Erik Mathiassen</i>	

Theoretical Work

Provable Security against Differential and Linear Cryptanalysis for the SPN Structure	273
<i>Seokhie Hong, Sangjin Lee, Jongin Lim, Jaechul Sung, Donghyeon Cheon, and Inho Cho</i>	

Unforgeable Encryption and Chosen Ciphertext Secure Modes of Operation	284
<i>Jonathan Katz and Moti Yung</i>	

Efficient Methods for Generating MARS-Like S-Boxes	300
<i>L. Burnett, G. Carter, E. Dawson, and W. Millan</i>	

Author Index	315
---------------------------	-----