Lecture Notes in Computer Science 1978

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

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

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

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 proceeedings, and I'll see everyone next year in Japan.

August 2000 Bruce Schneier

Table of Contents

General Stream-Cipher Cryptanalysis

AES Cryptanalysis 2

Block-Cipher Cryptanalysis 2

Theoretical Work