Lecture Notes in Computer Science 1039
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Dieter Gollmann (Ed.)

Fast Software Encryption

Third International Workshop
Cambridge, UK, February 21-23, 1996
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Dieter Gollmann
Royal Holloway, University of London, Department of Computer Science
Egham TW20 0EX, Surry, UK

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fast software encryption : ... international workshop ; proceedings. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer
3. Cambridge, UK, February 21 - 23, 1996. - 1996
(Lecture notes in computer science ; Vol. 1039)
ISBN 3-540-60865-6
NE: GT

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

ISBN 3-540-60865-6 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10512546 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This workshop on fast software encryption is the third in a series of meetings, which started in Cambridge two years ago, moved to Leuven last year, and has now returned to Cambridge. This time, the workshop has found a place in the programme on computer security, cryptology, and coding theory at the Isaac Newton Institute. It has grown from an invitational workshop to a meeting open to the general research community organised in association with the IACR.

The first workshop on fast software encryption set out with the aim to create a forum for discussing the engineering requirements in the design of fast cryptographic algorithms. As a necessary complement, it also included contributions on the actual analysis of cipher systems. We have been able to maintain the distinctive character and practical outlook of the workshops in this year's programme.

Block ciphers play a prominent part during the entire workshop. The first session on the analysis of block ciphers picks up on systems presented at previous workshops. Success in the analysis of those systems should set the scene for the remainder of the workshop and instill the constructive scepticism required in the design and evaluation of cryptographic algorithms. We will return to block ciphers in a session dedicated to proposals of new algorithms. The final session on design criteria is an apt conclusion to the workshop, suggesting ways forward for the work which will hopefully contribute to next year's meeting.

Hash functions have established themselves as a permanent fixture in the workshops on fast software encryption and we have been fortunate to attract a particularly interesting set of contributions on this topic. Again, we start with presentations of the analysis of algorithms and then move from the cryptanalysis of MD4 to proposals for fast and secure hash functions.

In the area of stream ciphers, there is one presentation of a pseudo-random generator and, in keeping with the tradition of previous workshops, a session on correlation analysis. In this session, the emphasis is on papers with direct implications on the practical analysis of stream ciphers.

I am indebted to the members of the Programme Committee for their detailed and helpful reviews. Even faced with very short reviewing deadlines, volunteers were prepared to look at papers beyond their allocated lot. Of course, I have to thank the authors for their contributions, which are essential to the success of the workshop, and for the timely submission of their final papers, which made the editor's job so much easier.

December 1995

Dieter Gollmann
Royal Holloway
University of London

The Isaac Newton Institute Research Programme

The Isaac Newton Institute is the UK's main centre for advanced research in the mathematical sciences. It is situated on the edge of the university town of Cambridge and, although formally part of Cambridge University, it is run as a national institute. It hosts six-month research programmes on topics which cut across the traditional boundaries of disciplines to bring together research workers with very different backgrounds and expertise; one of its most important goals is to overcome the barriers to research which are presented by departmental structures in universities.

The Institute asked me to organise a programme from January to June 1996 in computer security, cryptology, and coding theory. These closely related disciplines are concerned with assuring the dependability of computer and communications systems in the presence of noise and of opponents. They employ a number of related mathematical and engineering techniques; they are also a critical facilitating technology for a growing number of applications, ranging from payment networks through satellite TV and mobile communications to the construction of dependable distributed computer systems.

About eighty leading researchers in the field will be resident at the Institute, with the average stay about a month and a half and thus with about twenty people in residence at any one time. The program starts at the mathematical end of the subject and works towards more practical topics; its progression is from coding theory through cryptography and computational number theory to crypto protocols, computer security, and finally to security engineering.

For most of the time, the programme's function is to enable the participants to get away from their day-to-day commitments in an environment designed to facilitate collaborative research. However, during its course there are a number of more public events. These include weekly seminars which communicate the state of the art to the local research community, and three international scientific conferences. This volume is the proceedings of the first of these conferences, which deals with fast software encryption.

We are grateful to the many bodies whose financial support for the Institute has made the programme possible, including the UK Engineering and Physical Sciences Research Council, Trinity College, and St John's College. We are also grateful to the staff at the Isaac Newton Institute who are doing most of the organisational work for the conference.

December 1995

Ross Anderson
Computer Laboratory
University of Cambridge

Programme Committee

Ross Anderson	University of Cambridge, UK
Eli Biham	Technion, Haifa, Israel
Don Coppersmith	IBM T.J. Watson Research Center, USA
Cunsheng Ding	University of Turku, Finland
Dieter Gollmann	Royal Holloway, University of London, UK
James L. Massey	ETH Zürich, Switzerland
Mitsuru Matsui	Mitsubishi Electric Corporation, Japan
Bart Preneel	Katholieke Universiteit Leuven, Belgium

Contents

Block Ciphers – Analysis

Attacks on the HKM/HFX Cryptosystem 1
Xuejia Lai and Rainer A. Rueppel

Truncated Differentials of SAFER 15
Lars R. Knudsen and Thomas A. Berson

On the Weak Keys of Blowfish 27
Serge Vaudenay

Applications

High-Bandwidth Encryption with Low-Bandwidth Smartcards 33
Matt Blaze

ISAAC 41
Robert J. Jenkins Jr.

Hash Functions

A Note on the Hash Function of Tillich and Zémor 51
Willi Geiselmann

Cryptanalysis of MD4 53
Hans Dobbertin

RIPEMD-160: A Strengthened Version of RIPEMD 71
Hans Dobbertin, Antoon Bosselaers, and Bart Preneel

Fast Accumulated Hashing 83
Kaisa Nyberg

Tiger: A Fast New Hash Function 89
Ross Anderson and Eli Biham

Block Ciphers – Proposals

The Cipher SHARK 99
Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers, and Erik De Win

Two Practical and Provably Secure Block Ciphers: BEAR and LION 113
Ross Anderson and Eli Biham

Unbalanced Feistel Networks and Block Cipher Design 121
Bruce Schneier and John Kelsey

Correlation Analysis

A Comparison of Fast Correlation Attacks 145
Andrew Clark, Jovan Dj. Golić, and Ed Dawson

Correlation Attacks on Stream Ciphers:
Computing Low-Weight Parity Checks Based on Error-Correcting Codes . 159
Walter T. Penzhorn

On the Security of Nonlinear Filter Generators 173
Jovan Dj. Golić

Block Ciphers – Design Criteria

Faster Luby-Rackoff Ciphers 189
Stefan Lucks

New Structure of Block Ciphers with Provable Security Against
Differential and Linear Cryptanalysis 205
Mitsuru Matsui

List of Authors 219