Lecture Notes in Computer Science 1025
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Colin Boyd (Ed.)

Cryptography and Coding

5th IMA Conference
Cirencester, UK, December 18-20, 1995
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

Colin Boyd
The Manchester School of Engineering
Oxford Road, M13 9PL, Manchester, UK

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Cryptography and coding : 5th IMA conference, Cirencester, UK, December 18 - 20, 1995 ; proceedings / Colin Boyd (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1995
(Lecture notes in computer science ; Vol. 1025)
ISBN 3-540-60693-9
NE: Boyd, Colin [Hrsg.]; GT

CR Subject Classification (1991): E.3-4, G.2.1, C.2, J.1

1991 Mathematics Subject Classification: 11T71, 68P25, 94A60, 94Bxx

ISBN 3-540-60693-9 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10512350 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The first IMA Conference on Cryptography and Coding took place in December 1986. The second conference had to wait another three years, but since December 1989 the series has become bi-annual. The topics of cryptography and coding are inextricably linked; indeed the modern theories of both have their roots in the seminal work of Shannon. This conference is perhaps unique in concentrating on both areas and provides a valuable opportunity to explore the fruitful relationships between the two; many of the papers in this volume are concerned with the overlap.

This time there was a record of 48 papers submitted for inclusion. These were from an international authorship composed as follows: UK (27 submissions), France (4), Japan (2), Norway (2), Russia (2), Spain (2), Australia, Belgium, Germany, Italy, Malta, South Africa, Switzerland, USA, Yugoslavia. I would like to thank the authors of all papers, both those whose work is included in these Proceedings, and those whose work could not be accommodated. Without their months of research and painful writing up there would be no conference. As well as contributed papers we have been fortunate to enlist six eminent researchers to talk on particularly relevant topics of their choice.

The record number of submitted papers put an additional strain on the committee members. I am very grateful to them all for their work in assessing the papers in a short time and for freely giving me the benefit of their experience and support in a variety of ways. They are: Mike Darnell (University of Leeds), Paddy Farrell (University of Manchester), Mick Ganley (Racal Airtech) John Gordon (Concept Laboratories), Chris Mitchell (Royal Holloway), Fred Piper (Royal Holloway), Michael Walker (Vodaphone). I would also like to thank Pamela Bye, IMA Conference Officer, who dealt with all correspondence with the authors and was always ready to give advice and assistance.

The papers in this volume are presented in the order that they are intended to appear in the conference programme. As has become traditional at this conference, papers are not divided into related groups but are 'randomly' mixed.

Colin Boyd
Manchester, October 1995

Contents