Lecture Notes in Computer Science 2898

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

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Kenneth G. Paterson (Ed.)

Cryptography and Coding

9th IMA International Conference
Cirencester, UK, December 16-18, 2003
Proceedings

Springer

Volume Editor

Kenneth G. Paterson
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
E-mail: kenny.paterson@rhul.ac.uk

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): E.3-4, G.2.1, C.2, J.1

ISSN 0302-9743
ISBN 3-540-20663-9 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10966013 06/3142 5 4 3 2 1 0

Preface

The ninth in the series of IMA Conferences on Cryptography and Coding was held (as ever) at the Royal Agricultural College, Cirencester, from 16–18 December 2003. The conference's varied programme of 4 invited and 25 contributed papers is represented in this volume.

The contributed papers were selected from the 49 submissions using a careful refereeing process. The contributed and invited papers are grouped into 5 topics: coding and applications; applications of coding in cryptography; cryptography; cryptanalysis; and network security and protocols. These topic headings represent the breadth of activity in the areas of coding, cryptography and communications, and the rich interplay between these areas.

Assembling the conference programme and this proceedings required the help of many individuals. I would like to record my appreciation of them here.

Firstly, I would like to thank the programme committee who aided me immensely by evaluating the submissions, providing detailed written feedback for the authors of many of the papers, and advising me at many critical points during the process. Their help and cooperation was essential, especially in view of the short amount of time available to conduct the reviewing task. The committee this year consisted of Mike Darnell, Mick Ganley, Bahram Honary, Chris Mitchell, Matthew Parker, Nigel Smart and Mike Walker.

I would also like to thank those people who assisted the programme committee by acting as "secondary reviewers": Simon Blackburn, Colin Boyd, Alex Dent, Steven Galbraith, Keith Martin, James McKee, Sean Murphy, Dan Page, Matt Robshaw and Frederik Vercauteren. My apologies to any individuals missing from this list.

I am indebted to our four invited speakers for their contributions to the conference and this volume. The best candidates for invited speakers are always the most in-demand, and therefore busiest, people. This year's were no exception. Their contributions provided a valuable framing for the contributed papers.

My thanks too to the many authors who submitted papers to the conference. We were blessed this year with a strong set of submissions, and some good papers had to be rejected. I appreciate the understanding and good grace of those authors who were not successful with their submissions. I trust that they found any feedback from the reviewing process useful in helping to improve their work.

I am also grateful to the authors of accepted papers for their cooperation in compiling this volume: almost all of them met the various tight deadlines imposed by the production schedule. I would like to thank the staff at Springer-Verlag for their help with the production of this volume, especially Alfred Hofmann who answered many questions.

Much assistance was provided by Pamela Bye and Lucy Nye at the IMA. Their help took away much of the administrative burden, allowing the programme committee to focus on the scientific issues.

Valuable sponsorship for the conference was received from Hewlett-Packard Laboratories, Vodafone and the IEEE UKRI Communications Chapter.

Finally, I would like to thank my partner Liz for all her support during what was a very busy professional period for us both.

I Liz, Diolch o galon a llawer o gariad.

October 2003 Kenneth G. Paterson

Table of Contents

Coding and Applications

Applications of Coding in Cryptography

Cryptography

Cryptanalysis

Network Security and Protocols