

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

1025

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

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 1995

Printed in Germany

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 (Vodafone). 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

Design Choices and Security Implications in Implementing Diffie-Hellman Key Agreement (Invited Talk)	1
<i>Paul C. van Oorschot (Bell-Northern Research, Ottawa)</i>	
A Broadcast Key Distribution Scheme Based on Block Designs	2
<i>Valeri Korjik, Michael Ivkov, Yuri Merinovich, (St.Petersburg University of Telecommunications) Alexander Barg, Henk C.A. van Tilborg (Eindhoven University of Technology)</i>	
Minimal Supports in Linear Codes (Abstract)	13
<i>Alexei Ashikhmin (Delft University of Technology), Alexander Barg (Eindhoven University of Technology)</i>	
Sequential Decoding for a Subcode of Reed Solomon Codes	14
<i>Sooyoung Kim Shin, Peter Sweeney (University of Surrey)</i>	
Linear Span Analysis of a Set of Periodic Sequence Generators	22
<i>P. Caballero-Gil (University of La Laguna), A. Fúster-Sabater (CSIC, Madrid)</i>	
Minimal Weight k-SR Representations	34
<i>Yongfei Han, Dieter Gollmann, Chris Mitchell (University of London)</i>	
The Main Conjecture for MDS Codes (Invited Talk)	44
<i>J.W.P. Hirschfeld (University of Sussex)</i>	
Some Decoding Applications of Minimal Realization	53
<i>Graham Norton (University of Bristol)</i>	
The Synthesis of Perfect Sequences	63
<i>P.Z. Fan, M. Darnell (University of Leeds)</i>	
Computation of Low-Weight Parity Checks for Correlation Attacks on Stream Ciphers	74
<i>W.T. Penzhorn, G.J. Kühn (University of Pretoria)</i>	
A Storage Complexity Based Analogue of Maurer Key Establishment Using Public Channels	84
<i>C.J. Mitchell (University of London)</i>	
Soft Decision Decoding of Reed Solomon Codes Using the Dorsch Algorithm	94
<i>H.P. Ho, P. Sweeney (University of Surrey)</i>	

Good Codes Based on Very Sparse Matrices	100
<i>David J.C. MacKay (University of Cambridge), Radford M. Neal (University of Toronto)</i>	
Quantum Cryptography: Protecting our Future Networks with Quantum Mechanics (Invited Talk)	112
<i>Simon J.D. Phoenix, Paul D. Townsend (BT Laboratories)</i>	
Prepaid Electronic Cheques Using Public-Key Certificates	132
<i>Cristian Radu, René Govaerts, Joos Vandewalle (Katholieke Universiteit Leuven)</i>	
How Traveling Salespersons Prove Their Identity	142
<i>Stefan Lucks (Georg-August-Universität, Göttingen)</i>	
An Elliptic Curve Analogue of McCurley's Key Agreement Scheme	150
<i>Andrew Smith, Colin Boyd (University of Manchester)</i>	
Multi-Dimensional Ring TCM Codes for Fading Channels	158
<i>M. Ahmadian-Attari, P.G. Farrell (University of Manchester)</i>	
Authentication Codes: an Area where Coding and Cryptology Meet (Invited Talk)	169
<i>Henk C.A. van Tilborg (Eindhoven University of Technology)</i>	
Efficient Generation of Binary Words of Given Weight	184
<i>Nicolas Sendrier (INRIA)</i>	
Distribution of Recurrent Sequences Modulo Prime Powers (Abstract)	188
<i>Richard G.E. Pinch (University of Cambridge)</i>	
On-Line Secret Sharing	190
<i>Christian Cachin (ETH Zürich)</i>	
Church-Rosser Codes	199
<i>Vladimir A. Oleshchuk (Agder College, Grimstad)</i>	
A New Algorithm for Finding Minimum-Weight Words in Large Linear Codes	205
<i>Anne Canteaut (INRIA Projet Codes)</i>	
Coding and Cryptography for Speech and Vision (Invited Talk)	213
<i>E. V. Stansfield (Racal Research), M. Walker (Vodafone)</i>	
Some Constructions of Generalised Concatenated Codes Based on Unit Memory Codes (Invited Talk)	237
<i>Victor Zyablov (Institute for Problems of Information Transmission, Moscow), Sergo Shaugulidze (Georgian Technical University), Jorn Justesen (Technical University of Denmark)</i>	

A Note on the Hash Function of Tillich and Zémor	257
<i>Willi Geiselmann (University of London)</i>	
Cryptanalysis of Harari's Identification Scheme	264
<i>Pascal Véron (Université de Toulon et du Var)</i>	
Analysis of Sequence Segment Keying as a Method of CDMA Transmission	270
<i>T.M. Quirke, M. Darnell (University of Leeds)</i>	
Constructions for Variable-Length Error-Correcting Codes	282
<i>Victor Buttigieg (University of Malta), Patrick G. Farrell (University of Manchester)</i>	