

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Michael Walker (Ed.)

Cryptography and Coding

7th IMA International Conference
Cirencester, UK, December 20-22, 1999
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Michael Walker
Vodafone Limited
The Courtyard, 2-4 London Road
Newbury, Berkshire RG14 1JX, UK
E-mail: mike.walker@vf.vodafone.co.uk

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Cryptography and coding : ... IMA international conference ... ; proceedings. -
5[?]-. - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Singapore ; Tokyo : Springer, 1995[?]-
(Lecture notes in computer science ; ...)

7. Cirencester, UK, December 20 - 22, 1999. - 1999
(Lecture notes in computer science ; 1746)
ISBN 3-540-66887-X

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

ISSN 0302-9743
ISBN 3-540-66887-X 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 1999
Printed in Germany

Typesetting: Camera-ready by author
SPIN: 10750021 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

The IMA conferences on Cryptography and Coding are not only a blend of these two aspects of information theory, but a blend of mathematics and engineering and of theoretical results and applications. The papers in this book show that the 1999 conference was no exception. Indeed, we again saw the mathematics underlying cryptography and error correcting coding being applied to other aspects of communications, and we also saw classical mathematical concepts finding new applications in communications theory.

As usual the conference was held at the Royal Agricultural College, Cirencester, shortly before Christmas - this time 20-22 December 1999. The papers appear in this book in the order in which they were presented, grouped into sessions, each session beginning with an invited paper. These invited papers were intended to reflect the invitees' views on the future of their subject - or more accurately where they intended to take it. Indeed the focus of the conference was the *future of cryptography and coding* as seen through the eyes of young researchers.

The first group of papers is concerned with mathematical bounds, concepts, and constructions that form a common thread running through error correcting coding theory, cryptography, and codes for multiple access schemes. This is followed by a group of papers from a conference session concerned with applications. The papers range over various topics from arithmetic coding for data compression and encryption, through image coding, biometrics for authentication, and access to broadcast channels, to photographic signatures for secure identification. The third set of papers deals with theoretical aspects of error correcting coding, including graph and trellis decoding, turbo codes, convolution codes and low complexity soft decision decoding of Reed Solomon codes. This is followed by a collection of papers concerned with some mathematical techniques in cryptography - elliptic curves, the theory of correlations of binary sequences, primality testing, and the complexity of finite field arithmetic. The final collection of papers is concerned primarily with protocols and schemes. There is a diversity of papers covering lattice based cryptosystems, protocols for sharing public key parameters and for delegating decryption, and arithmetic coding schemes.

It is my pleasure to record my appreciation to the members of the conference organising committee for their help in refereeing the papers that make up this volume. They were Michael Darnell, Paddy Farrell, Mick Ganley, John Gordon, Bahram Honary, Chris Mitchell, and Fred Piper. Sincere thanks also to Pamela Bye, Hilary Hill, Adrian Lepper, and Deborah Sullivan of the IMA for all their help with the organisation of the conference and with the publication of this collection of papers.

Finally, I hope that those of you who attended the conference found it rewarding and stimulating. For those of you who did not, I hope this book of papers will encourage you to participate in the next one.

December 1999

Mike Walker

Contents

Applications of Exponential Sums in Communications Theory	1
<i>K.G. Paterson</i>	
Some Applications of Bounds for Designs to the Cryptography	25
<i>S. Nikova and V. Nikov</i>	
Further Results on the Relation Between Nonlinearity and Resiliency for Boolean Functions	35
<i>E. Pasalic and T. Johansson</i>	
Combinatorial Structure of Finite Fields with Two Dimensional Modulo Metrics	45
<i>E. Martínez-Moro, F.J. Galán-Simón, M.A. Borges-Trenard, and M. Borges-Quintana</i>	
A New Method for Generating Sets of Orthogonal Sequences for a Synchronous CDMA System	56
<i>H. Donelan and T. O'Farrell</i>	
New Self-Dual Codes over GF(5)	63
<i>S. Georgiou and C. Koukouvinos</i>	
Designs, Intersecting Families, and Weight of Boolean Functions	70
<i>E. Filiol</i>	
Coding Applications in Satellite Communication Systems	81
<i>S. McGrath</i>	
A Unified Code	84
<i>X. Liu, P. Farrell, and C. Boyd</i>	
Enhanced Image Coding for Noisy Channels	94
<i>P. Chippendale, C. Tanriover, and B. Honary</i>	
Perfectly Secure Authorization and Passive Identification for an Error Tolerant Biometric System	104
<i>G.I. Davida and Y. Frankel</i>	

An Encoding Scheme for Dual Level Access to Broadcasting Networks	114
<i>T. Amornraksa, D.R.B. Burgess, and P. Sweeney</i>	
Photograph Signatures for the Protection of Identification Documents	119
<i>B. Bellamy, J.S. Mason, and M. Ellis</i>	
An Overview of the Isoperimetric Method in Coding Theory	129
<i>J.-P. Tillich and G. Zémor</i>	
Rectangular Basis of a Linear Code	135
<i>J. Maucher, V. Sidorenko, and M. Bossert</i>	
Graph Decoding of Array Error-Correcting Codes	144
<i>P.G. Farrell and S.H. Razavi</i>	
Catastrophicity Test for Time-Varying Convolutional Encoders	153
<i>C. O'Donoghue and C. Burkley</i>	
Low Complexity Soft-Decision Sequential Decoding Using Hybrid Permutation for Reed-Solomon Codes	163
<i>M.-s. Oh and P. Sweeney</i>	
On Efficient Decoding of Alternant Codes over a Commutative Ring	173
<i>G.H. Norton and A. Sălăgean</i>	
Reduced Complexity Sliding Window BCJR Decoding Algorithms for Turbo Codes	179
<i>J. Gwak, S.K. Shin, and H.-M. Kim</i>	
Advanced Encryption Standard (AES) - An Update	185
<i>L.R. Knudsen</i>	
The Piling-Up Lemma and Dependent Random Variables	186
<i>Z. Kukorelly</i>	
A Cryptographic Application of Weil Descent	191
<i>S.D. Galbraith and N.P. Smart</i>	
Edit Probability Correlation Attack on the Bilateral Stop/Go Generator	201
<i>R. Menicocci and J.Dj. Golić</i>	

Look-Up Table Based Large Finite Field Multiplication in Memory Constrained Cryptosystems	213
<i>M.A. Hasan</i>	
On the Combined Fermat/Lucas Probable Prime Test	222
<i>S. Müller</i>	
On the Cryptanalysis of Nonlinear Sequences	236
<i>S.W. Golomb</i>	
Securing Aeronautical Telecommunications	243
<i>S. Blake-Wilson</i>	
Tensor-Based Trapdoors for CVP and Their Application to Public Key Cryptography	244
<i>R. Fischlin and J.-P. Seifert</i>	
Delegated Decryption	258
<i>Y. Mu, V. Varadharajan, and K.Q. Nguyen</i>	
Fast and Space-Efficient Adaptive Arithmetic Coding	270
<i>B. Ryabko and A. Fionov</i>	
Robust Protocol for Generating Shared RSA Parameters	280
<i>A.M. Barmawi, S. Takada, and N. Doi</i>	
Some Soft-Decision Decoding Algorithms for Reed-Solomon Codes	290
<i>S. Wesemeyer, P. Sweeney, and D.R.B. Burgess</i>	
Weaknesses in Shared RSA Key Generation Protocols	300
<i>S.R. Blackburn, S. Blake-Wilson, M. Burmester, and S.D. Galbraith</i>	
Digital Signature with Message Recovery and Authenticated Encryption (Signcryption) - A Comparison	307
<i>C.Y. Yeun</i>	
Index	313