

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

Series Editors

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

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

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 is a part of Springer Science+Business Media
springeronline.com

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

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

Recent Developments in Array Error-Control Codes	1
<i>Patrick Guy Farrell</i>	
High Rate Convolutional Codes with Optimal Cycle Weights	4
<i>Eirik Rosnes and Øyvind Ytrehus</i>	
A Multifunctional Turbo-Based Receiver Using Partial Unit Memory Codes	24
<i>Lina Fagoonee and Bahram Honary</i>	
Commitment Capacity of Discrete Memoryless Channels	35
<i>Andreas Winter, Anderson C.A. Nascimento, and Hideki Imai</i>	
Separating and Intersecting Properties of BCH and Kasami Codes	52
<i>Hans Georg Schaathun and Tor Helleseeth</i>	

Applications of Coding in Cryptography

Analysis and Design of Modern Stream Ciphers	66
<i>Thomas Johansson</i>	
Improved Fast Correlation Attack Using Low Rate Codes	67
<i>Håvard Molland, John Erik Mathiassen, and Tor Helleseeth</i>	
On the Covering Radius of Second Order Binary Reed-Muller Code in the Set of Resilient Boolean Functions	82
<i>Yuri Borissov, An Braeken, Svetla Nikova, and Bart Preneel</i>	
Degree Optimized Resilient Boolean Functions from Maiorana-McFarland Class	93
<i>Enes Pasalic</i>	
Differential Uniformity for Arrays	115
<i>K.J. Horadam</i>	

Cryptography

Uses and Abuses of Cryptography	125
<i>Richard Walton</i>	
A Designer's Guide to KEMs	133
<i>Alexander W. Dent</i>	

A General Construction of IND-CCA2 Secure Public Key Encryption	152
<i>Eike Kiltz and John Malone-Lee</i>	
Efficient Key Updating Signature Schemes Based on IBS	167
<i>Dae Hyun Yum and Pil Joong Lee</i>	
Periodic Sequences with Maximal Linear Complexity and Almost Maximal k -Error Linear Complexity	183
<i>Harald Niederreiter and Igor E. Shparlinski</i>	

Cryptanalysis

Estimates for Discrete Logarithm Computations in Finite Fields of Small Characteristic	190
<i>Robert Granger</i>	
Resolving Large Prime(s) Variants for Discrete Logarithm Computation	207
<i>A.J. Holt and J.H. Davenport</i>	
Computing the $M = UU^t$ Integer Matrix Decomposition	223
<i>Katharina Geißler and Nigel P. Smart</i>	
Cryptanalysis of the Public Key Cryptosystem Based on the Word Problem on the Grigorchuk Groups	234
<i>George Petrides</i>	
More Detail for a Combined Timing and Power Attack against Implementations of RSA	245
<i>Werner Schindler and Colin D. Walter</i>	
Predicting the Inversive Generator	264
<i>Simon R. Blackburn, Domingo Gomez-Perez, Jaime Gutierrez, and Igor E. Shparlinski</i>	
A Stochastic Model and Its Analysis for a Physical Random Number Generator Presented At CHES 2002	276
<i>Werner Schindler</i>	
Analysis of Double Block Length Hash Functions	290
<i>Mitsuhiko Hattori, Shoichi Hirose, and Susumu Yoshida</i>	

Network Security and Protocols

Cryptography in Wireless Standards (Invited Paper)	303
<i>Valtteri Niemi</i>	
On the Correctness of Security Proofs for the 3GPP Confidentiality and Integrity Algorithms	306
<i>Tetsu Iwata and Kaoru Kurosawa</i>	

A General Attack Model on Hash-Based Client Puzzles	319
<i>Geraint Price</i>	
Tripartite Authenticated Key Agreement Protocols from Pairings	332
<i>Sattam S. Al-Riyami and Kenneth G. Paterson</i>	
Remote User Authentication Using Public Information	360
<i>Chris J. Mitchell</i>	
Mental Poker Revisited	370
<i>Adam Barnett and Nigel P. Smart</i>	
Author Index	385