

Johannes Buchmann
Tom Høholdt
Henning Stichtenoth
Horacio Tapia-Recillas
Editors

Coding Theory, Cryptography and Related Areas

Proceedings of an International Conference
on Coding Theory, Cryptography and Related Areas,
held in Guanajuato, Mexico, in April 1998



Springer

Johannes Buchmann
Fachbereich Informatik
Technische Universität Darmstadt
Alexanderstrasse 10
64283 Darmstadt, Germany

Tom Høholdt
Department of Mathematics, Bldg. 303
Technical University of Denmark
2800 Lyngby, Denmark

Henning Stichtenoth
Fachbereich 6, Mathematik und Informatik
Universität Gesamthochschule Essen
45117 Essen, Germany

Horacio Tapia-Recillas
Departamento de Matemáticas
Universidad Autónoma Metropolitana-Iztapalapa
Apartado Postal 55-532, C.P.
09340 México, D. F., México

Library of Congress Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Coding theory, cryptography and related areas : proceedings of an
International Conference on Coding Theory, Cryptography and
Related Areas, held in Guanajuato, Mexico, in April 1998 / Johannes
Buchmann ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ;
Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer,
2000

ISBN 978-3-540-66248-8 ISBN 978-3-642-57189-3 (eBook)

DOI 10.1007/978-3-642-57189-3

Mathematics Subject Classification (1991): 11T71, 11Y16, 14C40, 94A60, 68P25, 12Fxx

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, reuse of illustrations, recitation, broadcasting, reproduction on microfilm 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 2000

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Cover design: *design & production* GmbH, Heidelberg

Typeset by the authors. Reformatted by Kurt Mattes, Heidelberg

Printed on acid-free paper SPIN 10716213 46/3143/LK - 5 4 3 2 1 0

Table of Contents

Modifications of the Rao-Nam Cryptosystem	1
<i>Ángela I. Barbero and Øyvind Ytrehus</i>	
Efficient Reduction on the Jacobian Variety of Picard Curves	13
<i>Ernesto Reinaldo Barreiro, Jorge Estrada Sarlabous, and Jean-Pierre Cherdieu</i>	
Continued Fractions in Hyperelliptic Function Fields	29
<i>T.G. Berry</i>	
Discrete Logarithms: Recent Progress	42
<i>Johannes Buchmann and Damian Weber</i>	
One-weight \mathbf{Z}_4 -linear Codes	57
<i>Claude Carlet</i>	
Efficient Algorithms for the Jacobian Variety of Hyperelliptic Curves $y^2 = x^p - x + 1$ Over a Finite Field of Odd Characteristic p	73
<i>Iwan Duursma and Kouichi Sakurai</i>	
On Weierstrass Semigroups and One-point Algebraic Geometry Codes	90
<i>J.I. Farrán</i>	
On the Undetected Error Probability of m -out-of- n Codes on the Binary Symmetric Channel	102
<i>Fang-Wei Fu, Torleiv Kløve, and Shu-Tao Xia</i>	
Skew Pyramids of Function Fields Are Asymptotically Bad	111
<i>Arnaldo Garcia and Henning Stichtenoth</i>	
A Public Key Cryptosystem Based on Sparse Polynomials	114
<i>D. Grant, K. Krastev, D. Lieman, and I. Shparlinski</i>	
Higher Weights of Grassmann Codes	122
<i>Sudhir R. Ghorpade and Gilles Lachaud</i>	
Toric Surfaces and Error-correcting Codes	132
<i>Johan P. Hansen</i>	
Decoding Spherical Codes Generated by Binary Partitions of Symmetric Pointsets	143
<i>John K. Karlof and Guodong Liu</i>	
Worst-Case Analysis of an Algorithm for Computing the Greatest Common Divisor of n Inputs	156
<i>Charles Lam, Jeffrey Shallit, and Scott Vanstone</i>	

Zeta Functions of Curves over Finite Fields with Many Rational Points . . .	167
<i>Kristin Lauter</i>	
Codes on Drinfeld Modular Curves	175
<i>Bartolomé López and Ignacio Luengo</i>	
Elliptic Curves, Pythagorean Triples and Applications	184
<i>J. Miret, J. Tena, and M. Valls</i>	
Exponential Sums and Stationary Phase (I)	195
<i>Carlos Julio Moreno</i>	
Exponential Sums in Several Variables over Finite Fields	209
<i>Oscar Moreno, Francis N. Castro, and Alberto Cáceres</i>	
Decoding Reed-Solomon Codes Beyond Half the Minimum Distance	221
<i>R. Refslund Nielsen and T. Høholdt</i>	
Reed-Muller Type Codes on the Veronese Variety over Finite Fields	237
<i>C. Rentería and H. Tapia-Recillas</i>	
Cryptography Primitives Based on a Cellular Automaton	244
<i>Jesús Urías</i>	
Factoring the Semigroup Determinant of a Finite Commutative Chain Ring	249
<i>Jay A. Wood</i>	