DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

Authentication Codes and Combinatorial Designs

Dingyi Pei

Chapman & Hall/CRC
Taylor & Francis Group
Boca Raton London New York

Published in 2006 by
Chapman & Hall/CRC
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 1-58488-473-8 (Hardcover)
International Standard Book Number-13: 978-1-58488-473-6 (Hardcover)
Library of Congress Card Number 2005026036

Library of Congress Cataloging-in-Publication Data

Pei, Dingyi.
Authentication codes and combinatorial designs / Dingyi Pei.
p. cm.
Includes bibliographical references and index.
ISBN 1-58488-473-8 (9781584884736)
1. Data encryption (Computer science) 2. Cryptography. 3. Combinatorial designs and configurations. I. Title.

QA76.9.A25P42 2005
005.8'2--dc22 2005026036

Contents

Preface **vii**

1 Introduction **1**
1.1 Authentication Problem 1
1.2 Authentication Schemes 3
1.3 Combinatorial Designs 5

2 Authentication Schemes **7**
2.1 Model with Three Participants (A-Codes) 7
2.2 Model with Four Participants (A^2-Codes) 10
2.3 Comments 13

3 Authentication Schemes with Three Participants **15**
3.1 Entropy 15
3.2 Information-Theoretic Bound 19
3.3 Perfect Authentication Schemes 21
3.4 Perfect Cartesian Codes 26
3.5 Combinatorial Bound 36
3.6 Comments 38
3.7 Exercises 39

4 Authentication Schemes with Arbitration **41**
4.1 Lower Bounds 41
4.2 Perfect Schemes with Arbitration 48
4.3 Perfect Cartesian A^2-Codes 56
4.4 Combinatorial Bounds of A^2-Codes 66
4.5 Comments 72
4.6 Exercises 73

5 A-Codes Based on Rational Normal Curves **75**
5.1 SPBD Based on RNC 75
5.2 A Family of Non-Cartesian Perfect A-Codes 80
5.3 Encoding Rules ($n = 2$, q Odd) 85
5.4 Encoding Rules ($n = 2$, q Even) 103
5.5 Comments 113
5.6 Exercises 113

6 t-Designs **115**
6.1 $2-(v,k,1)$ Designs 116
6.2 Steiner Triple System 117
6.3 $3-(v,k,1)$ Designs 122
6.4 Comments 124
6.5 Exercises 124

7 Orthogonal Arrays of Index Unity **127**
7.1 OA with Strength $t=2$ and Orthogonal Latin Squares . . . 127
7.2 Transversal Designs 135
7.3 Existence of $OA(n^2,4,n,2)$ 140
7.4 Bush's Construction 142
7.5 OA and Error-Correcting Codes 145
7.6 MDS Codes 147
7.7 Comments 150
7.8 Exercises 151

8 A-Codes from Finite Geometries **153**
8.1 Symplectic Spaces over Finite Fields 153
8.2 A-Codes from Symplectic Spaces 169
8.3 A-Codes from Unitary Spaces 178
8.4 Comments 182
8.5 Exercises 182

9 Authentication/Secrecy Schemes **185**
9.1 Perfect Secrecy Schemes 186
9.2 Construction of Perfect Secrecy Schemes 194
9.3 Authentication Schemes with Perfect Secrecy 204
9.4 Construction of Perfect Authentication/Secrecy Schemes . . 209
9.5 Comments 212
9.6 Exercises 213

Appendix: A Survey of Constructions for A-Codes **215**
A.1 Key Grouping Technique 215
A.2 Perpendicular Arrays 217
A.3 Generalized Quadrangles 221
A.4 Resolvable Block Design and A^2-Codes 226
A.5 Regular Bipartite Graphs 230

References **233**

Notations **237**