

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

© 2006 by Taylor & Francis Group, LLC  
Chapman & Hall/CRC is an imprint of Taylor & Francis Group

No claim to original U.S. Government works  
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

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

No part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access [www.copyright.com](http://www.copyright.com) (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC) 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

**Trademark Notice:** Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

---

### 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

---

**informa**

Taylor & Francis Group  
is the Academic Division of Informa plc.

Visit the Taylor & Francis Web site at  
<http://www.taylorandfrancis.com>

and the CRC Press Web site at  
<http://www.crcpress.com>

---

# Contents

<b>Preface</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Authentication Problem . . . . .	1
1.2 Authentication Schemes . . . . .	3
1.3 Combinatorial Designs . . . . .	5
<b>2 Authentication Schemes</b>	<b>7</b>
2.1 Model with Three Participants ( $A$ -Codes) . . . . .	7
2.2 Model with Four Participants ( $A^2$ -Codes) . . . . .	10
2.3 Comments . . . . .	13
<b>3 Authentication Schemes with Three Participants</b>	<b>15</b>
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
<b>4 Authentication Schemes with Arbitration</b>	<b>41</b>
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
<b>5 A-Codes Based on Rational Normal Curves</b>	<b>75</b>
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

<b>6</b>	<b>t-Designs</b>	<b>115</b>
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
<b>7</b>	<b>Orthogonal Arrays of Index Unity</b>	<b>127</b>
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
<b>8</b>	<b>A-Codes from Finite Geometries</b>	<b>153</b>
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
<b>9</b>	<b>Authentication/Secrecy Schemes</b>	<b>185</b>
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
	<b>Appendix: A Survey of Constructions for A-Codes</b>	<b>215</b>
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
	<b>References</b>	<b>233</b>
	<b>Notations</b>	<b>237</b>