

# Topics in Geometry, Coding Theory and Cryptography

*Edited by*

**Arnaldo Garcia**

*Instituto de Matematica Pura e Aplicada (IMPA),  
Rio de Janeiro, Brazil*

and

**Henning Stichtenoth**

*University of Duisburg-Essen, Germany and  
Sabanci University, Istanbul, Turkey*

 Springer

# Contents

Foreword	vii
1. Explicit Towers of Function Fields over Finite Fields <i>by A. Garcia and H. Stichtenoth</i>	1
1 Introduction	1
2 Towers and Codes	5
3 Genus and Splitting Rate of a Tower	16
4 Explicit Tame Towers	24
5 Explicit Wild Towers	31
6 Miscellaneous Results	47
References	55
2. Function Fields over Finite Fields and Their Applications to Cryptography <i>by H. Niederreiter, H. Wang and C. Xing</i>	59
1 Introduction	59
2 Applications to Combinatorial Cryptography	60
3 Applications to Stream Ciphers and Linear Complexity	89
References	99
3. Artin-Schreier Extensions and Their Applications <i>by C. Güneri and F. Özbudak</i>	105
1 Introduction	105
2 Artin-Schreier Extensions	107
3 Cyclic Codes and Their Weights	111
4 Trace Codes	120
5 Maximal Function Fields	126
References	130

4.	Pseudorandom Sequences <i>by A. Topuzođlu and A. Winterhof</i>	135
1	Introduction	135
2	Linear Complexity and Linear Complexity Profile	137
3	Autocorrelation and Related Distribution Measures for Binary Sequences	154
4	Discrepancy and Uniform Distribution	157
	References	162
5.	Group Structure of Elliptic Curves over Finite Fields and Applications <i>by R. Murty and I. Shparlinski</i>	167
1	Introduction	167
2	Group Structure	171
3	Applications to Cryptography	180
	References	187
	Appendix: Algebraic Function Fields	195
	About the Authors	199