

Lecture Notes Series, Institute for Mathematical Sciences,
National University of Singapore

Vol.
1

Editor **Harald Niederreiter**

CODING THEORY AND CRYPTOLOGY

Contents

Foreword	vii
Preface	ix
Extremal Problems of Coding Theory <i>A. Barg</i>	1
Analysis and Design Issues for Synchronous Stream Ciphers <i>E. Dawson and L. Simpson</i>	49
Quantum Error-Correcting Codes <i>K. Feng</i>	91
Public Key Infrastructures <i>D. Gollmann</i>	143
Computational Methods in Public Key Cryptology <i>A. K. Lenstra</i>	175
Detecting and Revoking Compromised Keys <i>T. Matsumoto</i>	239
Algebraic Function Fields Over Finite Fields <i>H. Niederreiter</i>	259
Authentication Schemes <i>D. Y. Pei</i>	283
Exponential Sums in Coding Theory, Cryptology and Algorithms <i>I. E. Shparlinski</i>	323

Distributed Authorization: Principles and Practice <i>V. Varadharajan</i>	385
Introduction to Algebraic Geometry Codes <i>C. P. Xing</i>	435