

Contents

Preface	vii
Cellular Automata in Stream Ciphers AMPARO FÚSTER-SABATER	1
Linear and Nonlinear Sequences and Applications to Stream Ciphers TOR HELLESETH	21
An Introduction to Pairing-Based Cryptography ALFRED MENEZES	47
Public-Key Cryptanalysis PHONG Q. NGUYEN	67
Pseudorandom Number Generators from Elliptic Curves IGOR E. SHPARLINSKI	121