

# Contents

Foreword	ix
Preface	xi
Approximate Counting with Uniform Constant-Depth Circuits MIKLÓS AJTAI	1
On Strong Separations from $AC^0$ ERIC ALLENDER AND VIVEK GORE	21
Parallel Matching Complexity of Ramsey’s Theorem JÓZSEF BECK	39
On Algorithms for Simple Stochastic Games ANNE CONDON	51
Locally Random Reductions in Interactive Complexity Theory JOAN FEIGENBAUM	73
An Application of Game-Theoretic Techniques to Cryptography MICHAEL J. FISCHER AND REBECCA N. WRIGHT	99
Composition of the Universal Relation JOHAN HÅSTAD AND AVI WIGDERSON	119
Practical Perfect Cryptographic Security UELI M. MAURER	135
Fair Games against an All-Powerful Adversary RAFAIL OSTROVSKY, RAMARATHNAM VENKATESAN, AND MOTI YUNG	155
Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation C. P. SCHNORR	171
A New Lower Bound Theorem for Read-Only-Once Branching Programs and its Applications JANOS SIMON AND MARIO SZEGEDY	183
On the E-Isomorphism Problem JIE WANG	195