

Contents

Preface	vii
Generic properties of subgroups of free groups and finite presentations FRÉDÉRIQUE BASSINO, CYRIL NICAUD, AND PASCAL WEIL	1
A new multi-server scheme for private information retrieval CHI SING CHUM AND XIAOWEN ZHANG	45
On secret sharing protocols CHI SING CHUM, BENJAMIN FINE, ANJA I. S. MOLDENHAUER, GERHARD ROSENBERGER, AND XIAOWEN ZHANG	51
A verifiable secret sharing scheme using non-abelian groups MAGGIE E. HABEEB	79
Non-associative public-key cryptography ARKADIUS KALKA	85
Non-associative key establishment protocols and their implementation ARKADIUS KALKA AND MINA TEICHER	113
Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups DANIEL KÖNIG, MARKUS LOHREY, AND GEORG ZETZSCHE	129
On the Tits alternative for a class of finitely presented groups with a special focus on symbolic computations ANJA I. S. MOLDENHAUER, GERHARD ROSENBERGER, AND KRISTINA ROSENTHAL	145
Geometry of the conjugacy problem in lamplighter groups ANDREW SALE	171
A logspace solution to the word and conjugacy problem of generalized Baumslag-Solitar groups ARMIN WEISS	185
Cryptographic hash functions from sequences of lifted Paley graphs SERENA YUAN	213