

# CONTEMPORARY MATHEMATICS

---

582

## Computational and Combinatorial Group Theory and Cryptography

AMS Special Sessions:

Computational Algebra, Groups, and Applications

April 30–May 1, 2011

University of Nevada, Las Vegas, NV

Mathematical Aspects of Cryptography and Cyber Security

September 10–11, 2011

Cornell University, Ithaca, NY

Benjamin Fine

Delaram Kahrobaei

Gerhard Rosenberger

Editors



---

**American Mathematical Society**  
Providence, Rhode Island

## Contents

Preface	vii
Weyl Gröbner Basis Cryptosystems RASHID ALI AND MARTIN KREUZER	1
A New Look at Finitely Generated Metabelian Groups GILBERT BAUMSLAG, ROMAN MIKHAILOV, AND KENT E. ORR	21
<i>IA</i> -Automorphisms of Groups with Almost Constant Upper Central Series MARIANNA BONANOME, MARGARET H. DEAN, AND MARCOS ZYMAN	39
A Proposed Alternative to the Shamir Secret Sharing Scheme CHI SING CHUM, BENJAMIN FINE, GERHARD ROSENBERGER, AND XIAOWEN ZHANG	47
Improving Latin Square Based Secret Sharing Schemes CHI SING CHUM AND XIAOWEN ZHANG	51
A Hand-Computation Involving Surface Groups, the Reidemeister-Schreier Rewriting Process and Kurosh Subgroup Theorem ANTHONY E. CLEMENT	65
Adjunction of Roots in Exponential A-Groups MARGARET H. DEAN, STEPHEN MAJEWICZ, AND MARCOS ZYMAN	71
Logspace Computations in Coxeter Groups and Graph Groups VOLKER DIEKERT, JONATHAN KAUSCH, AND MARKUS LOHREY	77
Collection by Polynomials in Finite $p$ -groups BETTINA EICK	95
All Finite Generalized Tetrahedron Groups II BENJAMIN FINE, ALEXANDER HULPKE, AND GERHARD ROSENBERGER	105
The Classification of One Relator Limit Groups and the Surface Group Conjecture BENJAMIN FINE AND GERHARD ROSENBERGER	107
Discrimination and Separation in the Metabelian Variety ANTHONY M. GAGLIONE, SEYMOUR LIPSCHUTZ, AND DENNIS SPELLMAN	129

A Secret Sharing Scheme Based on Group Presentations and the Word Problem MAGGIE HABEEB, DELARAM KAHROBAEI, AND VLADIMIR SHPILRAIN	143
Authenticated Key Agreement with Key Re-Use in the Short Authenticated Strings Model STANISLAW JARECKI AND NITESH SAXENA	151
Publicly Verifiable Secret Sharing Using Non-Abelian Groups DELARAM KAHROBAEI AND ELIZABETH VIDAURRE	175
A Note on the Hyperbolicity of Strict Pride Groups MATTHIAS NEUMANN-BROSIG	181
An Algorithm to Express Words as a Product of Conjugates of Relators ELLEN ZILIAK	187