

Contents

Key agreement, the Algebraic Eraser TM , and lightweight cryptography IRIS ANSHEL, MICHAEL ANSHEL, DORIAN GOLDFELD, STEPHANE LEMIEUX	1
Designing Key Transport Protocols Using Combinatorial Group Theory G. BAUMSLAG, T. CAMPS, B. FINE, G. ROSENBERGER, AND X. XU	35
Geometric Key Establishment ARKADY BERENSTEIN AND LEON CHERNYAK	45
Using shifted conjugacy in braid-based cryptography PATRICK DEHORNOY	65
Length-based conjugacy search in the braid group DAVID GARBER, SHMUEL KAPLAN, MINA TEICHER, BOAZ TSABAN, AND UZI VISHNE	75
Towards Provable Security for Cryptographic Constructions Arising from Combinatorial Group Theory MARÍA ISABEL GONZÁLEZ VASCO, RAINER STEINWANDT, AND JORGE L. VILLAR	89
Constructions in public-key cryptography over matrix groups DIMA GRIGORIEV AND ILIA PONOMARENKO	103
A Practical Attack on the Root Problem in Braid Groups ANJA GROCH, DENNIS HOFHEINZ, AND RAINER STEINWANDT	121
An attack on a group-based cryptographic scheme DENNIS HOFHEINZ AND DOMINIQUE UNRUH	133
Algebraic Problems in Symmetric Cryptography: Two Recent Results on Highly Nonlinear Functions NILS GREGOR LEANDER	141
Inverting the Burau and Lawrence-Krammer Representations EONKYUNG LEE	153
A new key exchange protocol based on the decomposition problem VLADIMIR SHPILRAIN AND ALEXANDER USHAKOV	161
Using the subgroup membership search problem in public key cryptography VLADIMIR SHPILRAIN AND GABRIEL ZAPATA	169