

1. Record Nr.	UNINA9910817177003321
Titolo	Group theory, statistics, and cryptography : AMS Special Session, Combinatorial and Statistical Group Theory, April 12-13, 2003, New York University / / Alexei G. Myasnikov, Vladimir Shpilrain, editors
Pubbl/distr/stampa	Providence, Rhode Island : , : American Mathematical Society, , [2004] ©2004
ISBN	0-8218-7950-2
Descrizione fisica	1 online resource (186 p.)
Collana	Contemporary mathematics, , 0271-4132 ; ; 360
Disciplina	512/.2
Soggetti	Group theory Mathematical statistics Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	""Contents""; ""Preface""; ""On power- and commutation transitive, power commutative, and restricted Gromov groups""; ""Braid-based cryptography""; ""1. Background on braids""; ""1.1. Braid groups""; ""1.2. The greedy normal form""; ""1.3. Implementation of braids""; ""2. Braid-based schemes""; ""2.1. Key exchange""; ""2.2. Enciphering&#x2013;deciphering""; ""2.3. Authentication""; ""2.4. Signature""; ""3. Attacks against the braid schemes""; ""3.1. Solutions to the Conjugacy Problem""; ""3.2. Attacks based on length""; ""3.3. Attacks based on linear representations"" ""3.4. Are these attacks dangerous?""""4. Clues for further research""; ""4.1. Key generation""; ""4.2. Random drawing and security proofs""; ""4.3. Using braid words and braid reduction""; ""4.4. Hash functions""; ""4.5. Resorting to other braid problems""; ""5. Conclusion""; ""Discriminating and squarelike groups I: Axiomatics""; ""The density of small words in a free group is 0""; ""Braid groups and Aut(F₂) are not rigid""; ""On varieties of groups in which all periodic groups are abelian""; ""Subgroups of fully residually free groups: algorithmic problems""; ""1. Introduction"" ""2. Preliminaries""""3. Intersection of two finitely generated subgroups of FZ[t]""; ""4. Properties of intersections of finitely generated

subgroups of $FZ[t]$ "; ""5. Centralizers in finitely generated fully residually free groups""; ""6. Conjugacy problem in finitely generated subgroups of $FZ[t]$ ""; ""References""; ""Weak hyperbolicity and free constructions""; ""Some properties of the conjugacy class growth function""; ""Boundary test elements""; ""Geodesics in the braid group on three strands""; ""Remarks on the growth of inverse semigroups""
""Assessing security of some group based cryptosystems""
