

1. Record Nr.	UNINA9910826587203321
Titolo	Algorithmic problems of group theory, their complexity, and applications to cryptography // Delaram Kahrobaei, Vladimir Shpilrain, editors
Pubbl/distr/stampa	Providence, Rhode Island : , : American Mathematical Society, , 2015 ©2015
ISBN	1-4704-2263-8
Descrizione fisica	1 online resource (123 p.)
Collana	Contemporary Mathematics, , 1098-3627 ; ; 633
Classificazione	20-XX68-XX
Disciplina	652/.8015122
Soggetti	Group theory Noncommutative algebras Algorithms Data encryption (Computer science) Cryptography Algebra
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"AMS Special Session on Algorithmic Problems of Group Theory and Applications to Information Security, April 6-7, 2013, Boston College, Chestnut Hill, MA."--Cover. "AMS Special Session on Algorithmic Problems of Group Theory and Their Complexity, January 9-10, 2013, San Diego, CA."--Cover.
Nota di bibliografia	Includes bibliographical references at the end of each chapters.
Nota di contenuto	""Cover""; ""Title page""; ""Contents""; ""Preface""; ""Secret sharing using non-commutative groups and the shortlex order""; ""1. Introduction""; ""2. Formal Definition""; ""3. Shamira's Secret Sharing Scheme""; ""4. Secret Sharing Using Non-commutative Groups""; ""5. Updating Relators""; ""6. Conclusion""; ""References""; ""An algorithm that decides conjugacy in a certain generalized free product""; ""1. Introduction""; ""2. Preliminaries""; ""3. The Algorithm""; ""References""; ""Classification of automorphic conjugacy classes in the free group on two generators""; ""1. Introduction"" ""2. The graph $I?( )$ ""; ""3. Non-root classes""; ""4. Root classes""; ""5. Enumeration""; ""Appendix A. Table of automorphic conjugacy classes""; ""Appendix B. Number of automorphic conjugacy classes of

each type"; "Appendix C. Number of paths of each size";  
"Acknowledgement"; "References"; "On elementary free groups";  
"1. Introduction"; "2. The Tarski Problems and Elementary Free  
Groups"; "3. Surface Groups and Magnus's Theorem"; "4. Cyclic  
Centralizers and Commuting Elements"; "5. Hyperbolicity and Stable  
Hyperbolicity"; "6. The Retract Theorem and Turner Groups"  
"7. Conjugacy Separability of Elementary Free Groups"; "8. Tame  
Automorphisms of Elementary Free Groups"; "9. Faithful  
Representations in  $(2, \mathbb{C})$ "; "References"; "An application of a  
localized version of an axiom of Ian Chiswell"; "1. Introduction"; "2.  
Questions"; "References"; "A note on Stallings's pregroups"; "1.  
Introduction"; "2. Adds, Prees and Pregroups"; "3. Kushner's  
Generalization of a Pregroup. T2-prees"; "4. Axiom [GLS2]"; "5.  
Generalizations"; "References"; "A CCA secure cryptosystem using  
matrices over group rings"  
"1. Cramer-Shoup cryptosystem"; "2. A CCA-2 secure cryptosystem  
using matrices over group rings"; "3. Adaptive CCA security for  
matrices over group rings"; "References"; "The MOR cryptosystem  
and finite  $p$ -groups"; "1. Introduction"; "2. Definitions and  
notations"; "3. The MOR cryptosystem"; "4. MOR cryptosystems on  
finite  $p$ -groups using  $\alpha$ -automorphisms"; "5. The MOR  
cryptosystem and elementary abelian  $p$ -group"; "6. The extra-special  
 $p$ -groups and its automorphism group"; "7. MOR cryptosystems on  
finite  $p$ -groups using  $\beta$ -automorphisms"; "8. Conclusion"  
"4. Open problems"

---