1. Record Nr. UNINA9910822592103321

Titolo	Algebraic methods in cryptography : Special Session on Algebraic Cryptography at the Joint International Meeting of the AMS and the Deutsche Mathematiker-Vereinigung, June 16-19, 2005, Mainz, Germany : International Workshop on Algebraic Methods in Cryptography, November 17-19, 2005, Bochum, Germany / / Lothar Gerritzen [and four others], editors
Pubbl/distr/stampa	Providence, Rhode Island : , : American Mathematical Society, , [2006] ©2006
ISBN	0-8218-8097-7 0-8218-4037-1
Descrizione fisica	1 online resource (190 p.)
Collana	Contemporary mathematics, , 0271-4132 ; ; volume 418
Disciplina	652/.8
Soggetti	Algebra Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	""Length-based conjugacy search in the braid group""""""Towards Provable Security for Cryptographic Constructions Arising from Combinatorial Group Theory""; ""Constructions in public-key cryptography over matrix groups""; ""A Practical Attack on the Root Problem in Braid Groups""; ""An attack on a group-based cryptographic scheme""; ""Algebraic Problems in Symmetric Cryptography: Two Recent Results on Highly Nonlinear Functions""; ""Inverting the Burau and Lawrence-Krammer Representations""; ""A new key exchange protocol based on the decomposition problem"" ""Using the subgroup membership search problem in public key cryptography""