1. Record Nr.	UNINA9910813134103321
Titolo	Algebraic curves and finite fields : cryptography and other applications / / edited by Harald Niederreiter [and three others]
Pubbl/distr/stampa	Berlin, [Germany] ; ; Boston, [Massachusetts] : , : De Gruyter, , 2014 ©2014
ISBN	3-11-037955-4
Descrizione fisica	1 online resource (254 p.)
Collana	Radon Series on Computational and Applied Mathematics, , 1865-3707 ; ; Volume 16
Classificazione	SK 240
Disciplina	516.352
Soggetti	Curves, Algebraic
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 at the end of each chapters and index.
Nota di contenuto	Front matter -- Introduction -- Contents -- Generic Newton polygons for curves of given p-rank / Achter, Jeffrey D. / Pries, Rachel -- Good towers of function fields / Bassa, Alp / Beelen, Peter / Nguyen, Nhut -- Correlation-immune Boolean functions for easing counter measures to side-channel attacks / Carlet, Claude / Guilley, Sylvain -- The discrete logarithm problem with auxiliary inputs / Cheon, Jung Hee / Kim, Taechan / Song, Yongsoo -- Garden of curves with many automorphisms / Giulietti, Massimo / Korchmáros, Gábor -- Nonlinear shift registers - A survey and challenges / Helleseth, Tor -- Permutations of finite fields and uniform distribution modulo 1 / Pausinger, Florian / Topuzolu, Alev -- Semifields, relative difference sets, and bent functions / Pott, Alexander / Schmidt, Kai-Uwe / Zhou, Yue -- NTRU cryptosystem: Recent developments and emerging mathematical problems in finite polynomial rings / Steinfeld, Ron -- Analog of the Kronecker-Weber theorem in positive characteristic / Villa-Salvador, Gabriel D. -- Index -- Backmatter
Sommario/riassunto	Algebra and number theory have always been counted among the most beautiful and fundamental mathematical areas with deep proofs and elegant results. However, for a long time they were not considered of any substantial importance for real-life applications. This has dramatically changed with the appearance of new topics such as

modern cryptography, coding theory, and wireless communication. Nowadays we find applications of algebra and number theory frequently in our daily life. We mention security and error detection for internet banking, check digit systems and the bar code, GPS and radar systems, pricing options at a stock market, and noise suppression on mobile phones as most common examples. This book collects the results of the workshops "Applications of algebraic curves" and "Applications of finite fields" of the RICAM Special Semester 2013. These workshops brought together the most prominent researchers in the area of finite fields and their applications around the world. They address old and new problems on curves and other aspects of finite fields, with emphasis on their diverse applications to many areas of pure and applied mathematics.