

1. Record Nr.	UNINA9910788632003321
Titolo	Arithmetic, geometry, cryptography, and coding theory 2009 : 12th Conference on Arithmetic, Geometry, Cryptography, and Coding Theory, March 30-April 3, 2009, Marseille, France : Geocrypt Conference, April 27-May 1, 2009, Pointe-a-Pitre, Guadeloupe, France : European Science Foundation Exploratory Workshop, Curves, Coding Theory, and Cryptography, March 25-29, 2009, Marseille, France // David Kohel, Robert Rolland, editors
Pubbl/distr/stampa	Providence, Rhode Island : , : American Mathematical Society, , [2010] ©2010
ISBN	0-8218-8200-7 0-8218-4955-7
Descrizione fisica	1 online resource (178 p.)
Collana	Contemporary mathematics, ; 521 , 0271-4132
Disciplina	516.3/5
Soggetti	Arithmetical algebraic geometry Abelian varieties Coding theory 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	Differentially 4-uniform functions / Yves Aubry and Francois Rodier -- Computing Hironaka's variants : Ridge and directrix / Jeremy Berthomieu, Pascal Hivert and Hussein Mourta -- Nondegenerate curves of low genus over small finite fields / Wouter Castryck and John Voight -- Faster side-channel resistant elliptic curve scalar multiplication / Alexandre Venelli and Francois Dassance -- Non linearite des fonctions booleennes donnees par des polynomes de degre binaire 3 definies sur $F[\text{subscript } 2m]$ avec $m$ pair / Eric Ferard and Francois Rodier -- A note on a maximal curve / Arnaldo Garcia and Henning Stichtenoth -- Computing Humbert surfaces and applications / David Gruenewald -- Genus 3 curves with many involutions and application to maximal curves in characteristic 2 / Enric Nart and Christophe Ritzenthaler -- Uniqueness of low genus optimal

curves over  $F$  / Alessandra Rigato -- Group order formulas for  
reductions of CM elliptic curves / Alice Silverberg -- Families of  
explicit isogenies of hyperelliptic Jacobians / Benjamin Smith --  
Computing congruences of modular forms and Galois representations  
modulo prime powers / Xavier Taixes i Ventosa and Gabor Wiese.

---