1.

Record Nr.	UNISA996465339603316
Titolo	Pairing-based cryptography - Pairing 2008 : second international conference, Egham, UK, September 1-3, 2008 ; proceedings / / Steven D. Galbraith, Kenneth G. Paterson (eds.)
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2008] ©2008
ISBN	3-540-85538-6
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XI, 377 p.)
Collana	Security and Cryptology ; ; 5209
Classificazione	54.62
Disciplina	005.82
Soggetti	Computer security Sets of pairs of functions to be distinguished Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Invited Talks -- Pairings in Trusted Computing -- Pairing Lattices -- The Uber-Assumption Family -- Cryptography I -- Homomorphic Encryption and Signatures from Vector Decomposition -- Hidden-Vector Encryption with Groups of Prime Order -- Mathematics -- The Hidden Root Problem -- Evaluating Large Degree Isogenies and Applications to Pairing Based Cryptography -- Computing the Cassels Pairing on Kolyvagin Classes in the Shafarevich-Tate Group -- Constructing Pairing Friendly Curves -- Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field -- Constructing Pairing-Friendly Elliptic Curves Using Factorization of Cyclotomic Polynomials -- A Generalized Brezing-Weng Algorithm for Constructing Pairing-Friendly Ordinary Abelian Varieties -- Pairing-Friendly Hyperelliptic Curves with Ordinary Jacobians of Type y 2?=?x 5?+?ax -- Implementation of Pairings -- Integer Variable ?–Based Ate Pairing -- Pairing Computation on Twisted Edwards Form Elliptic Curves -- Exponentiation in Pairing-Friendly Groups Using Homomorphisms -- Generators for the ?-Torsion Subgroup of Jacobians of Genus Two Curves -- Speeding Up Pairing Computations on Genus 2 Hyperelliptic Curves with Efficiently Computable Automorphisms -- Pairings on Hyperelliptic Curves with a Real Model

-- Hardware Implementation -- Faster Implementation of ? T Pairing over GF(3 m) Using Minimum Number of Logical Instructions for GF(3)-Addition -- A Comparison between Hardware Accelerators for the Modified Tate Pairing over and -- Cryptography II -- One-Round ID-Based Blind Signature Scheme without ROS Assumption -- Tracing Malicious Proxies in Proxy Re-encryption -- Security and Anonymity of Identity-Based Encryption with Multiple Trusted Authorities.

Sommario/riassunto

This book constitutes the thoroughly refereed proceedings of the Second International Conference on Pairing-Based Cryptography, Pairing 2008, held in London, UK, in September 2008. The 20 full papers, presented together with the contributions resulting from 3 invited talks, were carefully reviewed and selected from 50 submissions. The contents are organized in topical sections on cryptography, mathematics, constructing pairing-friendly curves, implementation of pairings, and hardware implementation.