1.	Record Nr.	UNINA9910484143503321
	Titolo	Pairing-Based Cryptography - Pairing 2007 : First International Conference, Pairing 2007, Tokyo, Japan, July 2-4, 2007, Proceedings / / edited by Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, Takeshi Okamoto
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
	ISBN	3-540-73489-9
	Edizione	[1st ed. 2007.]
	Descrizione fisica	1 online resource (XIII, 410 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 4575
	Disciplina	005.8
	Soggetti	Coding theory Information theory Cryptography Data encryption (Computer science) Algorithms Computer science - Mathematics Discrete mathematics Coding and Information Theory Cryptology Discrete Mathematics in Computer Science Symbolic and Algebraic Manipulation
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	Invited Talk I -- Bilinear Groups of Composite Order -- Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System -- Practical Time Capsule Signatures in the Standard Model from Bilinear Maps -- Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys -- Certificateless Public Key Encryption in the Selective-ID Security Model (Without Random Oracles) -- General and Efficient Certificateless Public Key Encryption Constructions -- Invited Talk II -- Hyperelliptic Pairings -- Zeta Function and Cryptographic Exponent of Supersingular Curves of Genus 2 -- Constructing Pairing-Friendly Genus 2 Curves with

Ordinary Jacobians -- Invited Talk III -- Implementing Cryptographic Pairings over Barreto-Naehrig Curves -- Instruction Set Extensions for Pairing-Based Cryptography -- The Importance of the Final Exponentiation in Pairings When Considering Fault Attacks -- Protocol I -- Proxy Re-encryption Systems for Identity-Based Encryption -- Fair Blind Signatures Revisited -- Invited Talk IV -- Supersingular Elliptic Curves in Cryptography -- On the Minimal Embedding Field -- Remarks on Cheon’s Algorithms for Pairing-Related Problems -- Invited Talk V -- On Pairing Inversion Problems -- The Tate Pairing Via Elliptic Nets -- Eta Pairing Computation on General Divisors over Hyperelliptic Curves y 2?=?x 7???x ±1 -- Protocol II -- Provably Secure Pairing-Based Convertible Undeniable Signature with Short Signature Length -- Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key.

Sommario/riassunto

Pairing-based cryptography is at the very leading edge of the current wave in computer cryptography. That makes this book all the more relevant, being as it is the refereed proceedings of the First International Conference on Pairing-Based Cryptography, Pairing 2007, held in Tokyo, Japan in 2007. The 18 revised full papers presented together were carefully reviewed and selected from 86 submissions. The papers are organized in topical sections including those on applications, and certificateless public key encryption.