1. Record Nr. UNINA9910484681403321

Titolo	Pairing-Based Cryptography--Pairing 2010 : 4th International Conference, Yamanaka Hot Spring, Japan, December 2010. proceedings / / Marc Joye, Atsuko Miyaji, Akira Otsuka, (eds.)
Pubbl/distr/stampa	Berlin ; ; New York, : Springer, 2010
ISBN	1-280-39056-5 9786613568489 3-642-17455-8
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XIII, 467 p. 37 illus.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 6487
Altri autori (Persone)	JoyeMarc MiyajiAtsuka OtsukaAkira
Disciplina	005.8/2
Soggetti	Cryptography Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Efficient Software Implementation -- An Analysis of Affine Coordinates for Pairing Computation -- High-Speed Software Implementation of the Optimal Ate Pairing over Barreto–Naehrig Curves -- Invited Talk 1 -- Some Security Topics with Possible Applications for Pairing-Based Cryptography -- Digital Signatures -- A New Construction of Designated Confirmer Signature and Its Application to Optimistic Fair Exchange -- Anonymizable Signature and Its Construction from Pairings -- Identification of Multiple Invalid Pairing-Based Signatures in Constrained Batches -- Cryptographic Protocols -- Oblivious Transfer with Access Control : Realizing Disjunction without Duplication -- Increased Resilience in Threshold Cryptography: Sharing a Secret with Devices That Cannot Store Shares -- Shorter Verifier-Local Revocation Group Signature with Backward Unlinkability -- Key Agreement -- Strongly Secure Two-Pass Attribute-Based Authenticated Key Exchange -- Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key Agreement -- Ephemeral Key Leakage Resilient and Efficient ID-AKEs That Can Share Identities, Private and Master Keys --