1. Record Nr. UNINA9910484681403321

Titolo	Pairing-Based Cryptography - Pairing 2010 : 4th International Conference, Yamanaka Hot Spring, Japan, December 13-15, 2010, Proceedings / / edited by Marc Joye, Atsuko Miyaji, Akira Otsuka
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : 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	Security and Cryptology, , 2946-1863 ; ; 6487
Altri autori (Persone)	JoyeMarc MiyajiAtsuka OtsukaAkira
Disciplina	005.8/2
Soggetti	Cryptography Data encryption (Computer science) Computer science - Mathematics Discrete mathematics Coding theory Information theory Computer networks Algorithms Data protection Cryptology Discrete Mathematics in Computer Science Coding and Information Theory Computer Communication Networks Data and Information 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 -- Invited Talk 2 -- Pairing-Based Non-interactive Zero-Knowledge Proofs -- Applications: Code Generation, Time-Released Encryption, Cloud Computing -- Designing a Code Generator for Pairing Based Cryptographic Functions -- Efficient Generic Constructions of Timed-Release Encryption with Pre-open Capability -- Optimal Authenticated Data Structures with Multilinear Forms -- Point Encoding and Pairing-Friendly Curves -- Deterministic Encoding and Hashing to Odd Hyperelliptic Curves -- Encoding Points on Hyperelliptic Curves over Finite Fields in Deterministic Polynomial Time -- A New Method for Constructing Pairing-Friendly Abelian Surfaces -- Generating MoreKawazoe-Takahashi Genus 2 Pairing-Friendly Hyperelliptic Curves -- ID-Based Encryption Schemes -- New Identity-Based Proxy Re-encryption Schemes to Prevent Collusion Attacks -- Fully Secure Anonymous HIBE and Secret-Key Anonymous IBE with Short Ciphertexts -- Chosen-Ciphertext Secure Identity-Based Encryption from Computational Bilinear Diffie-Hellman -- Invited Talk 3 -- A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties -- Efficient Hardware, FPGAs, and Algorithms -- Compact Hardware for Computing the Tate Pairing over 128-Bit-Security Supersingular Curves -- A Variant of Miller’s Formula and Algorithm -- Pairing Computation on Elliptic Curves with Efficiently Computable Endomorphism and Small Embedding Degree -- High Speed Flexible Pairing Cryptoprocessor on FPGA Platform.

Sommario/riassunto

The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R & D community, with numerous individuals, as well as with prestigious organizations and societies, LNCS has grown into the most comprehensive computer science research forum available. The scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes proceedings (published in time for the respective conference) post-proceedings (consisting of thoroughly revised final full papers) research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.) More recently, several color-cover sublines have been added featuring, beyond a collection of papers, various added-value components; these sublines include tutorials (textbook-like monographs or collections of lectures given at advanced courses) state-of-the-art surveys (offering complete and mediated coverage of a topic) hot topics (introducing emergent topics to the broader community) Book jacket.