1. Record Nr. UNISA996465838203316

Titolo	Pairing-Based Cryptography - Pairing 2009 [[electronic resource]] : Third International Conference Palo Alto, CA, USA, August 12-14, 2009 Proceedings / / edited by Hovav Shacham, Brent Waters
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	1-280-38315-1 9786613561077 3-642-03298-2
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (X, 267 p.)
Collana	Security and Cryptology ; ; 5671
Classificazione	DAT 465f SS 4800
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer programming Algorithms Computer science—Mathematics Data structures (Computer science) Cryptology Programming Techniques Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Data Structures and Information Theory Symbolic and Algebraic Manipulation Kongress. Palo Alto (Calif., 2009)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Signature Security -- Boneh-Boyen Signatures and the Strong Diffie-Hellman Problem -- Security of Verifiably Encrypted Signatures and a Construction without Random Oracles -- Multisignatures as Secure as the Diffie-Hellman Problem in the Plain Public-Key Model -- Curves -- On the Security of Pairing-Friendly Abelian Varieties over Non-prime

Fields -- Generating Pairing-Friendly Curves with the CM Equation of Degree 1 -- Pairing Computation -- On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves -- Faster Pairings on Special Weierstrass Curves -- Fast Hashing to G 2 on Pairing-Friendly Curves -- NIZKs and Applications -- Compact E-Cash and Simulatable VRFs Revisited -- Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures -- Group Signatures -- Identity Based Group Signatures from Hierarchical Identity-Based Encryption -- Forward-Secure Group Signatures from Pairings -- Efficient Traceable Signatures in the Standard Model -- Protocols -- Strongly Secure Certificateless Key Agreement -- Universally Composable Adaptive Priced Oblivious Transfer -- Conjunctive Broadcast and Attribute-Based Encryption.

Sommario/riassunto

This book constitutes the refereed proceedings of the Third International Conference on Pairing-Based Cryptography, Pairing 2009, held in Palo Alto, CA, USA, in August 2009. The 16 full papers presented were carefully reviewed and selected from 38 submissions. The papers are organized in topical sections on signature security, curves, pairing computation, non-interactive zero-knowledge systems and applications, group signatures, and protocols.