1. Record Nr. UNISA996465890703316

Titolo	Public Key Cryptography - PKC 2009 [[electronic resource]] : 12th International Conference on Practice and Theory in Public Key Cryptography Irvine, CA, USA, March 18-20, 2009, Proceedings / / edited by Stanislaw Jarecki, Gene Tsudik
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-00468-7
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XI, 521 p.)
Collana	Security and Cryptology ; ; 5443
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer communication systems Computer programming Algorithms Computers and civilization Management information systems Computer science Cryptology Computer Communication Networks Programming Techniques Algorithm Analysis and Problem Complexity Computers and Society Management of Computing and Information Systems
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	Number Theory -- Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint -- The Security of All Bits Using List Decoding -- A New Lattice Construction for Partial Key Exposure Attack for RSA -- Subset-Restricted Random Walks for Pollard rho Method on -- Applications and Protocols -- Signing a Linear Subspace: Signature Schemes for Network Coding -- Improving the Boneh-Franklin Traitor Tracing Scheme -- Modeling Key Compromise Impersonation Attacks

on Group Key Exchange Protocols -- Zero-Knowledge Proofs with Witness Elimination -- Multi-Party Protocols -- Distributed Public-Key Cryptography from Weak Secrets -- Asynchronous Multiparty Computation: Theory and Implementation -- Multi-Party Computation with Omnipresent Adversary -- Identity-Based Encryption -- Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data -- Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts -- Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys -- Removing Escrow from Identity-Based Encryption -- Signatures -- On the Theory and Practice of Personal Digital Signatures -- Security of Blind Signatures under Aborts -- Security of Sanitizable Signatures Revisited -- Identification of Multiple Invalid Signatures in Pairing-Based Batched Signatures -- Encryption -- CCA-Secure Proxy Re-encryption without Pairings -- Compact CCA-Secure Encryption for Messages of Arbitrary Length -- Verifiable Rotation of Homomorphic Encryptions -- New Cryptosystems and Optimizations -- A Practical Key Recovery Attack on Basic TCHo -- An Algebraic Surface Cryptosystem -- Fast Multibase Methods and Other Several Optimizations for Elliptic Curve Scalar Multiplication -- Group Signatures and Anonymous Credentials -- Revocable Group Signature Schemes with Constant Costs for Signing and Verifying -- An Accumulator Based on Bilinear Maps and Efficient Revocation for Anonymous Credentials -- Controlling Access to an Oblivious Database Using Stateful Anonymous Credentials.

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th International Conference on Practice and Theory in Public-Key Cryptography, PKC 2009, held in Irvine, CA, USA, in March 2009. The 28 revised full papers presented were carefully reviewed and selected from 112 submissions. The papers are organized in topical sections on number theory, applications and protocols, multi-party protocols, identity-based encryption, signatures, encryption, new cryptosystems and optimizations, as well as group signatures and anonymous credentials. .