1. Record Nr. UNINA9910483618603321

Titolo	Advances in cryptology -- EUROCRYPT 2008 : 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008 : proceedings / / Nigel Smart (ed.)
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2008] ©2008
ISBN	3-540-78967-7
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XIII, 564 p.)
Collana	Security and Cryptology ; ; 4965
Disciplina	005.82
Soggetti	Data transmission systems - Security measures Cryptography Computers - Access control
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	A Practical Attack on KeeLoq -- Key Recovery on Hidden Monomial Multivariate Schemes -- Predicting Lattice Reduction -- Efficient Sequential Aggregate Signed Data -- Proving Tight Security for Rabin-Williams Signatures -- Threshold RSA for Dynamic and Ad-Hoc Groups -- Towards Key-Dependent Message Security in the Standard Model -- The Twin Diffie-Hellman Problem and Applications -- Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products -- Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves -- On the Indifferentiability of the Sponge Construction -- A New Mode of Operation for Block Ciphers and Length-Preserving MACs -- Security/Efficiency Tradeoffs for Permutation-Based Hashing -- New Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5 -- Collisions for the LPS Expander Graph Hash Function -- Second Preimage Attacks on Dithered Hash Functions -- Efficient Two Party and Multi Party Computation Against Covert Adversaries -- Almost-Everywhere Secure Computation -- Truly Efficient 2-Round Perfectly Secure Message Transmission Scheme -- Protocols and Lower Bounds for Failure Localization in the Internet -- :

Increasing the Security and Efficiency of -- Sub-linear Zero-Knowledge Argument for Correctness of a Shuffle -- Precise Concurrent Zero Knowledge -- Efficient Non-interactive Proof Systems for Bilinear Groups -- Zero-Knowledge Sets with Short Proofs -- Strongly Multiplicative Ramp Schemes from High Degree Rational Points on Curves -- Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors -- Obfuscating Point Functions with Multibit Output -- Isolated Proofs of Knowledge and Isolated Zero Knowledge -- David and Goliath Commitments: UC Computation for Asymmetric Parties Using Tamper-Proof Hardware -- New Constructions for UC Secure Computation Using Tamper-Proof Hardware.

Sommario/riassunto

This book constitutes the refereed proceedings of the 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2008, held in Istanbul, Turkey, in April 2008. The 31 revised full papers presented were carefully reviewed and selected from 163 submissions. The papers address all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications. The papers are organized in topical sections on cryptanalysis, signatures, encryption, curve based cryptography, hash and mac function constructions, cryptanalysis of hash and mac functions, multi-party computation, protocols, zero knowledge, foundations, and UC multi-party computation using tamper proof hardware.