1. Record Nr. UNINA9910483707703321

Titolo	Advances in Cryptology – EUROCRYPT 2007 : 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings / / edited by Moni Naor
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	1-280-94372-6 9786610943722 3-540-72540-7
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (602 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4515
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer networks Data protection Algorithms Computer science - Mathematics Discrete mathematics Electronic data processing - Management Cryptology Computer Communication Networks Data and Information Security Discrete Mathematics in Computer Science IT Operations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities -- Non-trivial Black-Box Combiners for Collision-Resistant Hash-Functions Don’t Exist -- The Collision Intractability of MDC-2 in the Ideal-Cipher Model -- An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries --

Revisiting the Efficiency of Malicious Two-Party Computation -- Efficient Two-Party Secure Computation on Committed Inputs -- Universally Composable Multi-party Computation Using Tamper-Proof Hardware -- Generic and Practical Resettable Zero-Knowledge in the Bare Public-Key Model -- Instance-Dependent Verifiable Random Functions and Their Application to Simultaneous Resettability -- Conditional Computational Entropy, or Toward Separating Pseudoentropy from Compressibility -- Zero Knowledge and Soundness Are Symmetric -- Mesh Signatures -- The Power of Proofs-of-Possession: Securing Multiparty Signatures against Rogue-Key Attacks -- Batch Verification of Short Signatures -- Cryptanalysis of SFLASH with Slightly Modified Parameters -- Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy -- Secure Computation from Random Error Correcting Codes -- Round-Efficient Secure Computation in Point-to-Point Networks -- Atomic Secure Multi-party Multiplication with Low Communication -- Cryptanalysis of the Sidelnikov Cryptosystem -- Toward a Rigorous Variation of Coppersmith's Algorithm on Three Variables -- An L (1/3?+??) Algorithm for the Discrete Logarithm Problem for Low Degree Curves -- General Ad Hoc Encryption from Exponent Inversion IBE -- Non-interactive Proofs for Integer Multiplication -- Ate Pairing on Hyperelliptic Curves -- Ideal Multipartite Secret Sharing Schemes -- Non-wafer-Scale Sieving Hardware for the NFS: Another Attempt toCope with 1024-Bit -- Divisible E-Cash Systems Can Be Truly Anonymous -- A Fast and Key-Efficient Reduction of Chosen-Ciphertext to Known-Plaintext Security -- Range Extension for Weak PRFs; The Good, the Bad, and the Ugly -- Feistel Networks Made Public, and Applications -- Oblivious-Transfer Amplification -- Simulatable Adaptive Oblivious Transfer.

Sommario/riassunto

This book constitutes the refereed proceedings of the 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2007, held in Barcelona, Spain in May 2007. The 33 revised full papers presented were carefully reviewed and selected from 173 submissions. The papers address all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications.