1.	Record Nr.	UNINA9910768163803321
	Titolo	Advances in Cryptology - ASIACRYPT 2003 : 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003, Proceedings / / edited by Chi Sung Laih
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
	ISBN	3-540-40061-3
	Edizione	[1st ed. 2003.]
	Descrizione fisica	1 online resource (XIV, 550 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2894
	Disciplina	005.8
	Soggetti	Data encryption (Computer science) Coding theory Information theory Computer communication systems Operating systems (Computers) Algorithms Computer science—Mathematics Cryptology Coding and Information Theory Computer Communication Networks Operating Systems Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science
	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 at the end of each chapters and index.
	Nota di contenuto	Public Key Cryptography I -- Chosen-Ciphertext Security without Redundancy -- Some RSA-Based Encryption Schemes with Tight Security Reduction -- A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications -- Number Theory I -- Factoring Estimates for a 1024-Bit RSA Modulus -- Index Calculus Attack for Hyperelliptic Curves of Small Genus -- Efficient

Implementations -- Parallelizing Explicit Formula for Arithmetic in the Jacobian of Hyperelliptic Curves -- Tate Pairing Implementation for Hyperelliptic Curves y 2 = x p – x + d -- The AGM-X 0(N) Heegner Point Lifting Algorithm and Elliptic Curve Point Counting -- Key Management and Protocols -- Key Management Schemes for Stateless Receivers Based on Time Varying Heterogeneous Logical Key Hierarchy -- Leakage-Resilient Authenticated Key Establishment Protocols -- Untraceable Fair Network Payment Protocols with Off-Line TTP -- Hash Functions -- Incremental Multiset Hash Functions and Their Application to Memory Integrity Checking -- New Parallel Domain Extenders for UOWHF -- Cryptanalysis of 3-Pass HAVAL -- Group Signatures -- Efficient Group Signatures without Trapdoors -- Accumulating Composites and Improved Group Signing -- Almost Uniform Density of Power Residues and the Provable Security of ESIGN -- Number Theory II -- Rotations and Translations of Number Field Sieve Polynomials -- On Class Group Computations Using the Number Field Sieve -- Invited Talk -- The Secret and Beauty of Ancient Chinese Padlocks -- Block Ciphers -- A Traceable Block Cipher -- A New Attack against Khazad -- Broadcast and Multicast -- An Efficient Public Key Trace and Revoke Scheme Secure against Adaptive Chosen Ciphertext Attack -- Sequential Key Derivation Patterns for Broadcast Encryption and Key Predistribution Schemes -- Foundations and Complexity Theory -- Boneh et al.’s k-Element Aggregate Extraction Assumption Is Equivalent to the Diffie-Hellman Assumption -- On Diophantine Complexity and Statistical Zero-Knowledge Arguments -- Verifiable Homomorphic Oblivious Transfer and Private Equality Test -- Public Key Cryptography II -- Generalized Powering Functions and Their Application to Digital Signatures -- Certificateless Public Key Cryptography -- A Complete and Explicit Security Reduction Algorithm for RSA-Based Cryptosystems -- The Insecurity of Esign in Practical Implementations -- Digital Signature -- Efficient One-Time Proxy Signatures -- Universal Designated-Verifier Signatures.