1.	Record Nr.	UNISA996466256503316
	Titolo	Advances in Cryptology – EUROCRYPT 2002 [[electronic resource]] : International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002 Proceedings / / edited by Lars Knudsen
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
	ISBN	3-540-46035-7
	Edizione	[1st ed. 2002.]
	Descrizione fisica	1 online resource (XII, 552 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2332
	Disciplina	005.8
	Soggetti	Data encryption (Computer science) Coding theory Information theory Algorithms Computer science—Mathematics Management information systems Computer science Computer communication systems Cryptology Coding and Information Theory Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Management of Computing and Information Systems Computer Communication Networks
	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	Cryptanalysis I -- Cryptanalysis of a Pseudorandom Generator Based on Braid Groups -- Potential Weaknesses of the Commutator Key Agreement Protocol Based on Braid Groups -- Extending the GHS Weil Descent Attack -- Public-Key Encryption -- Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key

Encryption -- Key-Insulated Public Key Cryptosystems -- On the Security of Joint Signature and Encryption -- Invited Talk -- AES and the Wide Trail Design Strategy -- Information Theory & New Models -- Indistinguishability of Random Systems -- How to Fool an Unbounded Adversary with a Short Key -- Cryptography in an Unbounded Computational Model -- Implementational Analysis -- Performance Analysis and Parallel Implementation of Dedicated Hash Functions -- Fault Injection and a Timing Channel on an Analysis Technique -- Speeding Up Point Multiplication on Hyperelliptic Curves with Efficiently-Computable Endomorphisms -- Stream Ciphers -- Fast Correlation Attacks: An Algorithmic Point of View -- BDD-Based Cryptanalysis of Keystream Generators -- Linear Cryptanalysis of Bluetooth Stream Cipher -- Digital Signatures I -- Generic Lower Bounds for Root Extraction and Signature Schemes in General Groups -- Optimal Security Proofs for PSS and Other Signature Schemes -- Cryptanalysis II -- Cryptanalysis of SFLASH -- Cryptanalysis of the Revised NTRU Signature Scheme -- Key Exchange -- Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions -- Universally Composable Notions of Key Exchange and Secure Channels -- On Deniability in Quantum Key Exchange -- Modes of Operation -- A Practice-Oriented Treatment of Pseudorandom Number Generators -- A Block-Cipher Mode of Operation for Parallelizable Message Authentication -- Invited Talk -- Rethinking PKI: What’s Trust Got to Do with It? -- Digital Signatures II -- Efficient Generic Forward-Secure Signatures with an Unbounded Number of Time Periods -- From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security -- Security Notions for Unconditionally Secure Signature Schemes -- Traitor Tracking & Id-Based Encryption -- Traitor Tracing with Constant Transmission Rate -- Toward Hierarchical Identity-Based Encryption -- Multiparty and Multicast -- Unconditional Byzantine Agreement and Multi-party Computation Secure against Dishonest Minorities from Scratch -- Perfectly Secure Message Transmission Revisited -- Symmetric Cryptology -- Degree of Composition of Highly Nonlinear Functions and Applications to Higher Order Differential Cryptanalysis -- Security Flaws Induced by CBC Padding — Applications to SSL, IPSEC, WTLS...