1.

Record Nr.	UNISA996465613303316
Autore	Vadhan Salil
Titolo	Theory of cryptography : 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, the Netherlands, February 21-24, 2007 : proceedings / / Salil Vadhan
Pubbl/distr/stampa	Berlin : , : Springer, , [2007] ©2007
ISBN	1-280-90219-1 9786610902194 3-540-70936-3
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XI, 595 p.)
Collana	Lecture Notes in Computer Science ; ; Volume 4392
Altri autori (Persone)	VadhanSalil
Disciplina	005.8
Soggetti	Cryptography Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"International Association for Cryptologic Research"--Logo on cover.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Encryption I -- Does Privacy Require True Randomness? -- Tackling Adaptive Corruptions in Multicast Encryption Protocols -- Universally Composable Security -- Long-Term Security and Universal Composability -- Universally Composable Security with Global Setup -- Arguments and Zero Knowledge -- Parallel Repetition of Computationally Sound Protocols Revisited -- Lower Bounds for Non-interactive Zero-Knowledge -- Perfect NIZK with Adaptive Soundness -- Notions of Security -- Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries -- On the Necessity of Rewinding in Secure Multiparty Computation -- On Expected Probabilistic Polynomial-Time Adversaries: A Suggestion for Restricted Definitions and Their Benefits -- Obfuscation -- On Best-Possible Obfuscation -- Obfuscation for Cryptographic Purposes -- Securely Obfuscating Re-encryption -- Secret Sharing and Multiparty Computation -- Weakly-Private Secret Sharing Schemes -- On Secret Sharing Schemes, Matroids and Polymatroids -- Secure Linear Algebra Using Linearly Recurrent Sequences -- Towards Optimal and Efficient Perfectly Secure Message Transmission -- Signatures and Watermarking -- Concurrently-Secure

Blind Signatures Without Random Oracles or Setup Assumptions -- Designated Confirmer Signatures Revisited -- From Weak to Strong Watermarking -- Private Approximation and Black-Box Reductions -- Private Approximation of Clustering and Vertex Cover -- Robuster Combiners for Oblivious Transfer -- One-Way Permutations, Interactive Hashing and Statistically Hiding Commitments -- Towards a Separation of Semantic and CCA Security for Public Key Encryption -- Key Establishment -- Unifying Classical and Quantum Key Distillation -- Intrusion-Resilient Key Exchange in the Bounded Retrieval Model -- (Password) Authenticated Key Establishment: From 2-Party to Group -- Encryption II -- Multi-authority Attribute Based Encryption -- Conjunctive, Subset, and Range Queries on Encrypted Data -- How to Shuffle in Public -- Evaluating Branching Programs on Encrypted Data.