

1. Record Nr.	UNINA9910483713803321
Titolo	Automata, languages and programming : 33rd international colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006 : proceedings. Part II // Michele Bugliesi ... [et al.] (eds.)
Pubbl/distr/stampa	Berlin, : Springer, 2006
ISBN	3-540-35908-7
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XXIV, 612 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 4052 LNCS sublibrary. SL 1, Theoretical computer science and general issues Automata, languages and programming : 33rd international colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006 : proceedings ; ; pt. 2
Altri autori (Persone)	BugliesiMichele
Disciplina	004.0151
Soggetti	Machine theory Formal languages Computer programming
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 and index.
Nota di contenuto	Invited Papers -- Differential Privacy -- The One Way to Quantum Computation -- Zero-Knowledge and Signatures -- Efficient Zero Knowledge on the Internet -- Independent Zero-Knowledge Sets -- An Efficient Compiler from $\lambda$ -Protocol to 2-Move Deniable Zero-Knowledge -- New Extensions of Pairing-Based Signatures into Universal Designated Verifier Signatures -- Cryptographic Protocols -- Corrupting One vs. Corrupting Many: The Case of Broadcast and Multicast Encryption -- Cryptographically Sound Implementations for Communicating Processes -- A Dolev-Yao-Based Definition of Abuse-Free Protocols -- Secrecy and Protocol Analysis -- Preserving Secrecy Under Refinement -- Quantifying Information Leakage in Process Calculi -- Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or -- Cryptographic Primitives -- Generalized Compact Knapsacks Are Collision Resistant -- An Efficient Provable Distinguisher for HFE -- A Tight Bound for EMAC -- Constructing Single- and Multi-output Boolean Functions with Maximal Algebraic Immunity -- Bounded Storage and Quantum Models -- On Everlasting

Security in the Hybrid Bounded Storage Model -- On the Impossibility of Extracting Classical Randomness Using a Quantum Computer -- Quantum Hardcore Functions by Complexity-Theoretical Quantum List Decoding -- Foundations -- Efficient Pseudorandom Generators from Exponentially Hard One-Way Functions -- Hardness of Distinguishing the MSB or LSB of Secret Keys in Diffie-Hellman Schemes -- A Probabilistic Hoare-style Logic for Game-Based Cryptographic Proofs -- Multi-party Protocols -- Generic Construction of Hybrid Public Key Traitor Tracing with Full-Public-Traceability -- An Adaptively Secure Mix-Net Without Erasures -- Multipartite Secret Sharing by Bivariate Interpolation -- Identity-Based Encryption Gone Wild -- Games -- Deterministic Priority Mean-Payoff Games as Limits of Discounted Games -- Recursive Concurrent Stochastic Games -- Half-Positional Determinacy of Infinite Games -- A Game-Theoretic Approach to Deciding Higher-Order Matching -- Semantics -- Descriptive and Relative Completeness of Logics for Higher-Order Functions -- Interpreting Polymorphic FPC into Domain Theoretic Models of Parametric Polymorphism -- Typed Gol for Exponentials -- Commutative Locative Quantifiers for Multiplicative Linear Logic -- Automata I -- The Wadge Hierarchy of Deterministic Tree Languages -- Timed Petri Nets and Timed Automata: On the Discriminating Power of Zeno Sequences -- On Complexity of Grammars Related to the Safety Problem -- Models -- Jumbo  $\lambda$ -Calculus --  $\lambda$ -RBAC: Programming with Role-Based Access Control -- Communication of Two Stacks and Rewriting -- Equations -- On the Axiomatizability of Priority -- A Finite Equational Base for CCS with Left Merge and Communication Merge -- Theories of HNN-Extensions and Amalgamated Products -- On Intersection Problems for Polynomially Generated Sets -- Logics -- Invisible Safety of Distributed Protocols -- The Complexity of Enriched  $\lambda$ -Calculi -- Interpreting Tree-to-Tree Queries -- Automata II -- Constructing Exponential-Size Deterministic Zielonka Automata -- Flat Parametric Counter Automata -- Lower Bounds for Complementation of  $\lambda$ -Automata Via the Full Automata Technique.

---