1.	Record Nr.	UNISA996465909503316
	Titolo	Automata, Languages and Programming [[electronic resource]] : 35th International Colloquium, ICALP 2008 Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II / / edited by Luca Aceto, Ivan Damgaard, Leslie Ann Goldberg, Magnus M. Halldorsson, Anna Ingolfsdottir, Igor Walukiewicz
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
	ISBN	3-540-70583-X
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (XXII, 734 p.)
	Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 5126
	Disciplina	005.1
	Soggetti	Software engineering Computer programming Computer science Computer science—Mathematics Discrete mathematics Numerical analysis Artificial intelligence—Data processing Software Engineering Programming Techniques Theory of Computation Discrete Mathematics in Computer Science Numerical Analysis Data 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 and index.
	Nota di contenuto	Invited Lectures -- Composable Formal Security Analysis: Juggling Soundness, Simplicity and Efficiency -- Newton’s Method for ?-Continuous Semirings -- Track B: Logic, Semantics, and Theory of Programming -- The Tractability Frontier for NFA Minimization -- Finite Automata, Digraph Connectivity, and Regular Expression Size -- Leftist Grammars Are Non-primitive Recursive -- On the Computational

Completeness of Equations over Sets of Natural Numbers -- Placement Inference for a Client-Server Calculus -- Extended pi-Calculi -- Completeness and Logical Full Abstraction in Modal Logics for Typed Mobile Processes -- On the Sets of Real Numbers Recognized by Finite Automata in Multiple Bases -- On Expressiveness and Complexity in Real-Time Model Checking -- STORMED Hybrid Systems -- Controller Synthesis and Verification for Markov Decision Processes with Qualitative Branching Time Objectives -- On Datalog vs. LFP -- Directed st-Connectivity Is Not Expressible in Symmetric Datalog -- Non-dichotomies in Constraint Satisfaction Complexity -- Quantified Constraint Satisfaction and the Polynomially Generated Powers Property -- When Does Partial Commutative Closure Preserve Regularity? -- Weighted Logics for Nested Words and Algebraic Formal Power Series -- Tree Languages Defined in First-Order Logic with One Quantifier Alternation -- Duality and Equational Theory of Regular Languages -- Reversible Flowchart Languages and the Structured Reversible Program Theorem -- Attribute Grammars and Categorical Semantics -- A Domain Theoretic Model of Qubit Channels -- Interacting Quantum Observables -- Perpetuality for Full and Safe Composition (in a Constructive Setting) -- A System F with Call-by-Name Exceptions -- Linear Logical Algorithms -- A Simple Model of Separation Logic for Higher-Order Store -- Open Implication -- ATL* Satisfiability Is 2EXPTIME-Complete -- Visibly Pushdown Transducers -- The Non-deterministic Mostowski Hierarchy and Distance-Parity Automata -- Analyzing Context-Free Grammars Using an Incremental SAT Solver -- Track C: Security and Cryptography Foundations -- Weak Pseudorandom Functions in Minicrypt -- On Black-Box Ring Extraction and Integer Factorization -- Extractable Perfectly One-Way Functions -- Error-Tolerant Combiners for Oblivious Primitives -- Asynchronous Multi-Party Computation with Quadratic Communication -- Improved Garbled Circuit: Free XOR Gates and Applications -- Improving the Round Complexity of VSS in Point-to-Point Networks -- How to Protect Yourself without Perfect Shredding -- Universally Composable Undeniable Signature -- Interactive PCP -- Constant-Round Concurrent Non-malleable Zero Knowledge in the Bare Public-Key Model -- Delegating Capabilities in Predicate Encryption Systems -- Bounded Ciphertext Policy Attribute Based Encryption -- Making Classical Honest Verifier Zero Knowledge Protocols Secure against Quantum Attacks -- Composable Security in the Bounded-Quantum-Storage Model -- On the Strength of the Concatenated Hash Combiner When All the Hash Functions Are Weak -- History-Independent Cuckoo Hashing -- Building a Collision-Resistant Compression Function from Non-compressing Primitives -- Robust Multi-property Combiners for Hash Functions Revisited -- Homomorphic Encryption with CCA Security -- How to Encrypt with the LPN Problem -- Could SFLASH be Repaired? -- Password Mistyping in Two-Factor-Authenticated Key Exchange -- Affiliation-Hiding Envelope and Authentication Schemes with Efficient Support for Multiple Credentials.

Sommario/riassunto

The two-volume set LNCS 5125 and LNCS 5126 constitutes the refereed proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP 2008, held in Reykjavik, Iceland, in July 2008. The 126 revised full papers presented together with 4 invited lectures were carefully reviewed and selected from a total of 407 submissions. The papers are grouped in three major tracks on algorithms, automata, complexity and games, on logic, semantics, and theory of programming, and on security and cryptography foundations. LNCS 5126 contains 56 contributions of track B and track C selected from 208 submissions and 2 invited lectures. The papers for track B are

organized in topical sections on bounds, distributed computation, real-time and probabilistic systems, logic and complexity, words and trees, nonstandard models of computation, reasoning about computation, and verification. The papers of track C cover topics in security and cryptography such as theory, secure computation, two-party protocols and zero-knowledge, encryption with special properties/quantum cryptography, various types of hashing, as well as public-key cryptography and authentication.