

1. Record Nr.	UNISA996466466203316
Titolo	Algebraic Informatics [[electronic resource] ] : 6th International Conference, CAI 2015, Stuttgart, Germany, September 1-4, 2015. Proceedings // edited by Andreas Maletti
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-23021-2
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (VIII, 223 p. 21 illus.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 9270
Disciplina	004
Soggetti	Computer science Machine theory Cryptography Data encryption (Computer science) Computer science—Mathematics Discrete mathematics Software engineering Computer Science Logic and Foundations of Programming Formal Languages and Automata Theory Cryptology Discrete Mathematics in Computer Science Software Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Learning Weighted Automata -- More Than 1700 Years of Word Equations -- An Algebraic Geometric Approach to Multidimensional Words -- Why We Need Semirings in Automata Theory -- Unbordered Pictures: Properties and Construction -- Effective Invariant Theory of Permutation Groups using Representation Theory -- On differential uniformity of maps that may hide an algebraic trapdoor -- On the Lower Block Triangular Nature of the Incidence Matrices to Compute the Algebraic Immunity of Boolean Functions -- Weighted Unranked Tree Automata over Tree Valuation Monoids and Their Characterization

by Weighted Logics -- A New Partial Key Exposure Attack on Multi-power RSA -- A Chomsky-Schützenberger Theorem for Weighted Automata with Storage -- EF+EX Forest Algebras -- On near prime-order elliptic curves with small embedding degrees -- Key-Policy Multi-Authority Attribute-Based Encryption -- Extended Explicit Relations Between Trace, Definition Field, and Embedding Degree -- Complexity of Uniform Membership of Context-Free Tree Grammars -- Attacking BEAR and LION schemes in a realistic scenario -- Weighted Restarting Automata and Pushdown Relations -- Equivalence checking problem for finite state transducers over semigroups.

---

Sommario/riassunto

This book constitutes the refereed proceedings of the 6th International Conference on Algebraic Informatics, CAI 2015, held in Stuttgart, Germany, in September 2015. The 15 revised full papers presented were carefully reviewed and selected from 25 submissions. The papers cover topics such as data models and coding theory; fundamental aspects of cryptography and security; algebraic and stochastic models of computing; logic and program modelling.

---