Lecture Notes In Computer Science 5308

You are holding the rst in a hopefully long and successful series of RSA Cr- tographers' Track proceedings. The Cryptographers' Track (CT-RSA) is one of the many parallel tracks of the yearly RSA Conference. Other sessions deal with government projects, law and policy issues, freedom and privacy news, analysts' opinions, standards, ASPs, biotech and healthcare, nance, telecom and wireless security, developers, new products, implementers, threats, RSA products, VPNs, as well as cryp- graphy and enterprise tutorials. RSA Conference 2001 is expected to continue the tradition and remain the largest computer security event ever staged: 250 vendors, 10,000 visitors and 3,000 class-going attendees are expected in San Francisco next year. I am very grateful to the 22 members of the program committee for their hard work. The program committee received 65 submissions (one of which was later withdrawn) for which review was conducted electronically; almost all papers had at least two reviews although most had three or more. Eventually, we accepted the 33 papers that appear in these proceedings. Revisions were not checked on their scienti c aspects and some authors will write nal versions of their papers for publication in refereed journals. As is usual, authors bear full scienti c and paternity responsibilities for the contents of their papers.

This volume contains the proceedings of the Latin American Theoretical Inf- matics (LATIN) conference that was held in Buenos Aires, Argentina, April 5–8, 2004. The LATIN series of symposia was launched in 1992 to foster interactions between the Latin American community and computer scientists around the world. This was the sixth event in the series, following S ? ao Paulo, Brazil (1992), Valparaiso, Chile (1995), Campinas, Brazil (1998), Punta del Este, Uruguay (2000), and Cancun, Mexico (2002). The proceedings of these conferences were also published by Springer-Verlag in the Lecture Notes in Computer Science series: Volumes 583, 911, 1380, 1776, and 2286, respectively. Also, as before, we published a selection of the papers in a special issue of a prestigious journal. We received 178 submissions. Each paper was assigned to four program c- mittee members, and 59 papers were selected. This was 80% more than the previous record for the number of submissions. We feel lucky to have been able to build on the solid foundation provided by the increasingly successful previous LATINs. And we are very grateful for the tireless work of Pablo Mart ? ?nez L ? opez, the Local Arrangements Chair. Finally, we thank Springer-Verlag for publishing these proceedings in its LNCS series.

The two-volume set LNCS 9516 and 9517 constitutes the thoroughly refereed proceedings of the 22nd International Conference on Multimedia Modeling, MMM 2016, held in Miami, FL, USA, in January 2016. The 32 revised full papers and 52 poster papers were carefully reviewed and selected from 117 submissions. In addition 20 papers were accepted for five special sessions out of 38 submissions as well as 7 demonstrations (from 11 submissions) and 9 video showcase

papers. The papers are organized in topical sections on video content analysis, social media analysis, object recognition and system, multimedia retrieval and ranking, multimedia representation, machine learning in multimedia, and interaction and mobile. The special sessions are: good practices in multimedia modeling; semantics discovery from multimedia big data; perception, aesthetics, and emotion in multimedia quality modeling; multimodal learning and computing for human activity understanding; and perspectives on multimedia analytics./div

The book constitutes the joint refereed proceedings of the 10th International Conference on Relational Methods in Computer Science, RelMiCS 2008, and the 5th International Conference on Applications of Kleene Algebras, AKA 2008, held in Manchester, UK in April 2008. The 26 revised full papers presented together with 2 invited papers were carefully reviewed and selected from numerous submissions. The papers describe the calculus of relations and similar algebraic formalisms as methodological and conceptual tools with special focus on formal methods for software engineering, logics of programs and links to neighbouring disciplines. Their scope comprises relation algebra, fixpoint calculi, semiring theory, iteration algebras, process algebras and dynamic algebras. Applications include formal algebraic modeling, the semantics, analysis and development of programs, formal language theory and combinatorial optimization.

This open access book constitutes the proceedings of the 29th European Symposium on Programming, ESOP 2020, which was planned to take place in Dublin, Ireland, in April 2020, as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2020. The actual ETAPS 2020 meeting was postponed due to the Corona pandemic. The papers deal with fundamental issues in the specification, design, analysis, and implementation of programming languages and systems.

This book constitutes the refereed proceedings of the 34th Conference on Current Trends in Theory and Practice of Computer Science, SOFSEM 2008, held in Slovakia, in 2008. The 57 revised full papers, presented together with 10 invited contributions, were carefully reviewed and selected from 162 submissions. The contributions are segmented into four topical sections on foundations of computer science; computing by nature; networks, security, and cryptography; and Web technologies.

This volume brings together papers from various fields of theoretical computer science, including computational geometry, parallel algorithms, algorithms on graphs, data structures and complexity of algorithms. Some of the invited papers include surveys of results in particular fields and some report original research, while all the contributed papers report original research. Most of the algorithms given are for parallel models of computation. The papers were presented at the Second International Symposium on Optimal Algorithms held in Varna, Bulgaria, in May/June 1989. The volume will be useful to researchers and students in theoretical computer science, especially in parallel computing.

This book constitutes the refereed proceedings of the 44th International Conference on Current Trends in Theory and Practice of Computer Science, SOFSEM 2018, held in Krems, Austria, in January/February 2018. The 48 papers presented in this volume were carefully reviewed and selected from 97 submissions. They were organized in topical sections named: foundations of computer science; software engineering: advances methods, applications, and tools; data, information and knowledge engineering; network science and parameterized complexity; model-based software engineering; computational models and complexity; software quality assurance and transformation; graph structure and computation; business processes, protocols, and mobile networks; mobile robots and server systems; automata, complexity, completeness; recognition and generation; optimization, probabilistic analysis, and sorting; filters, configurations, and picture encoding; machine learning; text searching algorithms; and data model engineering.

This book constitutes the refereed proceedings of the 25th IFIP WG 6.1 International Conference on Formal Techniques for Networked and Distributed Systems, FORTE 2005, held in Taipei, Taiwan, in October 2005. The 33 revised full papers and 6 short papers presented together with 3 keynote speeches were carefully reviewed and selected from 88 submissions. The papers cover all current aspects of formal methods for distributed systems and communication protocols such as formal description techniques (MSC, UML, Use cases, . . .), semantic foundations, model-checking, SAT-based techniques, process algebrae, abstractions, protocol testing, protocol verification, network synthesis, security system analysis, network robustness, embedded systems, communication protocols, and several promising new techniques.

This book constitutes the refereed proceedings of the 22nd International Conference on DNA Computing and Molecular Programming, DNA 22, held Munich, Germany, in September 16 The 11 full papers presented together with 10 invited and tutorial talks were carefully selected from 55 submissions Research in DNA computing and molecular programming draws together mathematics, computer science, physics, chemistry, biology, and nanotechnology to address the analysis, design, and synthesis of information-based molecular systems

The papers in this volume were presented at the fourth biennial Summer Conference on Category Theory and Computer Science, held in Paris, September3-6, 1991. Category theory continues to be an important tool in foundationalstudies in computer science. It has been widely applied by logicians to get concise interpretations of many logical concepts. Links between logic and computer science have been developed now for over twenty years, notably via the Curry-Howard isomorphism which identifies programs with proofs and types with propositions. The triangle category theory - logic - programming presents a rich world of interconnections. Topics covered in this volume include the following. Type theory: stratification of types and propositions can be discussed in a categorical setting. Domain theory: synthetic domain theory

develops domain theory internally in the constructive universe of the effective topos. Linear logic: the reconstruction of logic based on propositions as resources leads to alternatives to traditional syntaxes. The proceedings of the previous three category theory conferences appear as Lecture Notes in Computer Science Volumes 240, 283 and 389.

This book constitutes the refereed proceedings of the 22nd Conference on Foundations of Software Technology and Theoretical Computer Science, FST TCS 2002, held in Kanpur, India in December 2002. The 26 revised full papers presented together with 5 invited contributions were carefully reviewed and selected from 108 submissions. A broad variety of topics from the theory of computing are addressed, from algorithmics and discrete mathematics as well as from logics and programming theory.

Lecture Notes in Computer ScienceAn Index and Other Useful InformationLecture Notes in Computer Science : 1-100Lecture Notes in Control and Computer ScienceMultiMedia Modeling22nd International Conference, MMM 2016, Miami, FL, USA, January 4-6, 2016, ProceedingsSpringer

This book constitutes the refereed proceedings of the 23rd Conference on Foundations of Software Technology and Theoretical Computer Science, FST TCS 2003, held in Mumbai, India in December 2003. The 23 revised full papers presented together with 4 invited papers and the abstract of an invited paper were carefully reviewed and selected from 160 submissions. A broad variety of current topics from the theory of computing are addressed, ranging from algorithmics and discrete mathematics to logics and programming theory.

This book is based on the author's Ph.D. thesis which was selected during the 1994 ACM Doctoral Dissertation Competition as one of the two co-winning works. T.V. Raman did his Ph.D. work at Cornell University with Professor Davied Gries as thesis advisor. The author presents the computing system ASTER that audio formats electronic documents to produce audio documents. ASTER can speak both literary texts and highly technical documents containing complex mathematics (presented in (LA)TEX).

This book constitutes the refereed proceedings of the 14th Algorithms and Data Structures Symposium, WADS 2015, held in Victoria, BC, Canada, August 2015. The 54 revised full papers presented in this volume were carefully reviewed and selected from 148 submissions. The Algorithms and Data Structures Symposium - WADS (formerly Workshop on Algorithms And Data Structures), which alternates with the Scandinavian Workshop on Algorithm Theory, is intended as a forum for researchers in the area of design and analysis of algorithms and data structures. WADS includes papers presenting original research on algorithms and data structures in all areas, including bioinformatics, combinatorics, computational geometry, databases, graphics, and parallel and distributed computing.

This two volume set LNCS 9827 and LNCS 9828 constitutes the refereed proceedings of the 27th International Conference on Database and Expert Systems Applications, DEXA 2016, held in Porto, Portugal, September 2016. The 39 revised full papers presented together with 29 short papers were carefully reviewed and selected from 137 submissions. The papers discuss a range

of topics including: Temporal, Spatial, and High Dimensional Databases; Data Mining; Authenticity, Privacy, Security, and Trust; Data Clustering; Distributed and Big Data Processing; Decision Support Systems, and Learning; Data Streams; Data Integration, and Interoperability; Semantic Web, and Data Semantics; Social Networks, and Network Analysis; Linked Data; Data Analysis; NoSQL, NewSQL; Multimedia Data; Personal Information Management; Semantic Web and Ontologies; Database and Information System Architectures; Query Answering and Optimization; Information Retrieval, and Keyword Search; Data Modelling, and Uncertainty.

This book describes the functional properties and the structural organization of the members of the thrombospondin gene family. These proteins comprise a family of extracellular calcium binding proteins that modulate cellular adhesion, migration and proliferation. Thrombospondin-1 has been shown to function during angiogenesis, wound healing and tumor cell metastasis.

This book constitutes the refereed proceedings of the 9th International Conference on Information Security, ISC 2006, held on Samos Island, Greece in August/September 2006. The 38 revised full papers presented were carefully reviewed and selected from 188 submissions. The papers are organized in topical sections.

This book constitutes the proceedings of the 14th International Conference on Relational and Algebraic Methods in Computer Science, RAMiCS 2014 held in Marienstatt, Germany, in April/May 2014. The 25 revised full papers presented were carefully selected from 37 submissions. The papers are structured in specific fields on concurrent Kleene algebras and related formalisms, reasoning about computations and programs, heterogeneous and categorical approaches, applications of relational and algebraic methods and developments related to modal logics and lattices.

This book constitutes the revised selected papers of the 44th International Workshop on Graph-Theoretic Concepts in Computer Science, WG 2018, held in Cottbus, Germany, in June 2018. The 30 full papers presented in this volume were carefully reviewed and selected from 66 submissions. They cover a wide range of areas, aiming at connecting theory and applications by demonstrating how graph-theoretic concepts can be applied in various areas of computer science. Another focus is on presenting recent results and on identifying and exploring promising directions of future research.

This volume contains selected papers from FCT '91. Topics covered include: semantics and logical concepts, automata and formal languages, computational geometry, complexity, algorithms, and counting and combinatorics.

This book features the refereed proceedings of the 2nd International Symposium on Computer Science in Russia held in September 2007. The 35 papers cover theory track deals with algorithms, protocols, and data structures; complexity and cryptography; formal languages, automata and their applications to computer science; computational models and concepts; proof theory; and applications of logic to computer science. Many applications are presented.

This double volume set (LNAI 10863-10864) constitutes the refereed proceedings of the 25th International Workshop, EG-ICE 2018, held in Lausanne, Switzerland, in June 2018. The 58 papers presented in this volume were carefully reviewed and selected from 108 submissions. The papers are organized in topical sections on Advanced Computing in Engineering, Computer Supported Construction Management, Life-Cycle Design Support, Monitoring and Control Algorithms in Engineering, and BIM and Engineering Ontologies.

This book constitutes the thoroughly refereed post-proceedings of the 11th International Workshop on Coalgebraic Methods in Computer Science, CMCS 2012, colocated with ETAPS 2012, held in Tallin, Estonia, in March/April 2012. The 10 revised full papers were carefully reviewed and selected from 23 submissions. Also included are three invited talks. The papers cover a wide range of topics in the theory, logics and applications of coalgebras.

The ability to draw inferences is a central operation in any artificial intelligence system. Automated reasoning is therefore among the traditional disciplines in AI. Theory reasoning is about techniques for combining automated reasoning systems with specialized and efficient modules for handling domain knowledge called background reasoners. Connection methods have proved to be a good choice for implementing high-speed automated reasoning systems. They are the starting point in this monograph,in which several theory reasoning versions are defined and related to each other. A major contribution of the book is a new technique of linear completion allowing for the automatic construction of background reasoners from a wide range of axiomatically given theories. The emphasis is on theoretical investigations, but implementation techniques based on Prolog are also covered.

Image-based rendering, as an area of overlap between computer graphics and computer vision, uses computer vision techniques to aid in sythesizing new views of scenes. Image-based rendering methods are having a substantial impact on the field of computer graphics, and also play an important role in the related field of multimedia systems, for applications such as teleconferencing, remote instruction and surgery, virtual reality and entertainment. The book develops a novel way of formalizing the view synthesis problem under the full perspective model, yielding a clean, linear warping equation. It shows new techniques for dealing with visibility issues such as partial occlusion and "holes". Furthermore, the author thoroughly re-evaluates the requirements that view synthesis places on stereo algorithms and introduces two novel stereo algorithms specifically tailored to the application of view synthesis.

The four-volume set LNCS 6765-6768 constitutes the refereed proceedings of the 6th International Conference on Universal Access in Human-Computer Interaction, UAHCI 2011, held as Part of HCI International 2011, in Orlando, FL, USA, in July 2011, jointly with 10 other conferences addressing the latest research and development efforts and highlighting the human aspects of design and use of computing systems. The 47 revised papers included in the third volume were carefully reviewed and selected from numerous submissions. The papers are organized in the following topical sections: universal access in the mobile context; ambient assisted living and smart environments; driving and interaction; interactive technologies in the physical and built environment.

Intelligent computing refers greatly to artificial intelligence with the aim at making computer to act as a human. This newly developed area of real-time intelligent computing integrates the aspect of dynamic environments with the human intelligence. This book presents a comprehensive practical and easy to read account which describes current state-of-the art in designing and implementing real-time intelligent computing to robotics, alert systems, IoT, remote access control, multi-agent systems, networking, mobile smart systems, crowd sourcing, broadband systems, cloud computing, streaming data and many other applications areas. The solutions discussed in this book will encourage the researchers and IT professional to put the methods into their practice.

The open access two-volume set LNCS 11561 and 11562 constitutes the refereed proceedings of the 31st International

Conference on Computer Aided Verification, CAV 2019, held in New York City, USA, in July 2019. The 52 full papers presented together with 13 tool papers and 2 case studies, were carefully reviewed and selected from 258 submissions. The papers were organized in the following topical sections: Part I: automata and timed systems; security and hyperproperties; synthesis; model checking; cyber-physical systems and machine learning; probabilistic systems, runtime techniques; dynamical, hybrid, and reactive systems; Part II: logics, decision procedures; and solvers; numerical programs; verification; distributed systems and networks; verification and invariants; and concurrency.

The Cryptographers' Track (CT-RSA) is a research conference within the RSA conference, the largest, regularly staged computer security event. CT-RSA 2004 was the fourth year of the Cryptographers' Track, and it is now an established venue for presenting practical research results related to cryptography and data security. The conference received 77 submissions, and the program committee sel- ted 28 of these for presentation. The program committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to cryp- graphy. Each paper was reviewed by at least three program committee members. Extended abstracts of the revised versions of these papers are in these proc- dings. The program also included two invited lectures by Dan Boneh and Silvio Micali. I am extremely grateful to the program committee members for their en- mous investment of time and e?ort in the di?cult and delicate process of review and selection. Many of them attended the program committee meeting during the Crypto 2003 conference at the University of California, Santa Barbara.

In an age of explosive worldwide growth of electronic data storage and communications, effective protection of information has become a critical requirement. When used in coordination with other tools for ensuring information security, cryptography in all of its applications, including data confidentiality, data integrity, and user authentication, is a most powerful tool for protecting information. This book presents a collection of research work in the field of cryptography. It discusses some of the critical challenges that are being faced by the current computing world and also describes some mechanisms to defend against these challenges. It is a valuable source of knowledge for researchers, engineers, graduate and doctoral students working in the field of cryptography. It will also be useful for faculty members of graduate schools and universities.

This volume commemorates Shimon Even, one of founding fathers of Computer Science in Israel, who passed away on May 1, 2004. This Festschrift contains research contributions, surveys and educational essays in theoretical computer science, written by former students and close collaborators of Shimon. The essays address natural computational problems and are accessible to most researchers in theoretical computer science.

This book constitutes the refereed proceedings of the 21st International Symposium on Mathematical Foundations of

Computer Science, MFCS '96, held in Crakow, Poland in September 1996. The volume presents 35 revised full papers selected from a total of 95 submissions together with 8 invited papers and 2 abstracts of invited talks. The papers included cover issues from the whole area of theoretical computer science, with a certain emphasis on mathematical and logical foundations. The 10 invited presentations are of particular value.

This book constitutes the refereed proceedings of the 19th International Workshop on Computer Science Logic, CSL 2005, held as the 14th Annual Conference of the EACSL in Oxford, UK in August 2005. The 33 revised full papers presented together with 4 invited contributions were carefully reviewed and selected from 108 papers submitted. All current aspects of logic in computer science are addressed ranging from mathematical logic and logical foundations to methodological issues and applications of logics in various computing contexts. The volume is organized in topical sections on semantics and logics, type theory and lambda calculus, linear logic and ludics, constraints, finite models, decidability and complexity, verification and model checking, constructive reasoning and computational mathematics, and implicit computational complexity and rewriting.