ICALP 2006

33rd International Colloquium on Automata, Languages and Programming

July 9-16, 2006 - S. Servolo, Venice – Italy

TECHNICAL PROGRAM

Main Conference
Satellite Workshops

EVENTS

ICALP'06 The 33rd International Colloquium on Automata, Languages and Programming

Held under the auspices of

European Association for Theoretical Computer Science
Mogens Nielsen, President
Jan van Leeuwen, Vice President
Paul Spirakis, Vice President

Program Committees

Track A

Ingo Wegener (Universität Dortmund, Germany - **PC Chair**)

Harry Buhrman (University of Amsterdam, The Netherlands)
Mark de Berg (TU Eindhoven, The Netherlands)
Uriel Feige (Weizmann Institute, Isreal)
Anna Gàl (University of Texas at Austin, USA)
Johan Hastad (KTH Stockholm, Sweden)
Edith Hemaspaandra (Rochester Institute of Technology, USA)
Kazuo Iwama (Kyoto University, Japan)
Mark Jerrum (University of Edinburgh, UK)
Stefano Leonardi (Università di Roma, Italy)
Friedhelm Meyer auf der Heide (Univrsität. Paderborn, Germany)
Ian Munro (University of Waterloo, Canada)
Sotiris Nikoletseas (Patras University, Greece)
Rasmus Pagh (IT Univerisy of Copenhagen, Denmark)
Tim Roughgarden (Stanford University, USA)
Jacques Sakarovitch (CRNS Paris, France)
Jiri Sgall (Academy of Sciences, Prague, Czech Republic)
Hans Ulrich Simon (Ruhr-Universität Bochum, Germany)
Alistair Sinclair (University of Berkeley, USA)
Angelika Steger (ETH Zürich, Switzerland)
Denis Thérien (McGill University, Canada)
Emo Welzl (ETH Zürich, Switzerland)

Track B

Vladimiro Sassone (Univerisity of Southampton, UK - **Chair**)

Roberto Amadio (Université Paris 7, France)
Lars Birkedal (IT University of Copenhagen, Denmark)
Roberto Bruni (Università di Pisa, Italy)
Mariangiola Dezani (Università di Torino, Italy)
Volker Diekert (University of Stuttgart, Germany)
Abbas Edalat (Imperial College, UK)
Jan Friso Groote Eindhoven University of Technology, The Nederlands
Tom Henzinger (EPFL, Switzerland)
Madhavan Mukund (Chennai Mathematical Institute, INDIA)
Jean-Éric Pin (L.I.A.F.A, France)
Julian Rathke (University of Sussex, UK)
Jakob Rehof (Microsoft Research, Redmont, USA)
Don Sannella (Univeriity of Edinburgh, UK)
Nicole Schweikardt (Humboldt-Universität zu Berlin, Germany)
Helmut Seidl (Technische Universität München, Germany)
Peter Selinger (Dalhousie University, Canada)
Jerzy Tiuryn (Warsaw University, Poland)
Victor Vianu (U. C. San Diego, USA)
David Walker (Princeton University, USA)
Igor Walukiewicz (Labri, Universitè Bordeaux, France)

Track C

Bart Preneel (Katholieke Universiteit Leuven, Belgium - **Chair**)

Martín Abadi (University of California at Santa Cruz, USA)
Christian Cachin (IBM Research, Switzerland)
Ronald Cramer (CWI and Leiden University, The Netherlands)
Ivan Damgård (University of Aarhus, Denmark)
Giovanni Di Crescenzo (Telcordia, USA)
Marc Fischlin (ETH Zürich, Switzerland)
Dieter Gollmann (University of Hamburg-Harburg, Germany)
Andrew D. Gordon (Microsoft Research, UK)
Aggelos Kiayias (University of Connecticut, USA)
Joe Kilian (Rutgers University, USA)
Cathy Meadows (Naval Research Laboratory, USA)
John Mitchell (Stanford University, USA)
Mats Näslund (Ericsson, Sweden)
Tatsuaki Okamoto (Kyoto University, Japan)
Rafael Ostrovksy (University of California at Los Angeles, USA)
Pascal Paillier (Gemplus, France)
Giuseppe Persiano (University of Salerno, Italy)
Benny Pinkas (HP Labs, Israel)
Vitaly Shmatikov (University of Texas at Austin, USA)
Victor Shoup (New York University, USA)

Jessica Staddon (PARC, USA)
Frederik Vercauteren (Katholieke Universiteit Leuven, Belgium)

Organizing Committee

Michele Bugliesi (Chair)
Andrea Pietracaprina (Stellite events)
Francesco Ranzato (Stellite events)
Sabina Rossi (Stellite events)
Annalisa Bossi
Damiano Macedonio

ICALP 2006 Satellite Workshops

ALGOSENSORS: Int, Workshop on Algorithmic Aspects of Wireless Sensor Networks

CHR: Third Workshop on Constraint Handling Rules

CL&C: Classical Logic and Computation

DCM: Second International Workshop on Developments in Computational Models

FCC: Formal and Computational Cryptography

iETA: Improving Exponential-Time Algorithms: Strategies and Limitations

MeCBIC: Membrane Computing and Biologically Inspired Process Calculi

SecReT: First International Workshop on Security and Rewriting Techniques

WCAN: Second Workshop on Cryptography for Ad Hoc Networks

EVENTS – SUMMARY

ICALP'06 Programme: Monday July 10, 2006

8.00 **Registration**

8:50 - 9:00 **ICALP'06 Opening**

9:00 - 10:00 **ICALP Invited Lecture** **Auditorium**

Additive Approximation for Edge-Deletion Problems

Alon Noga, Tel Aviv University, Israel

Chair: I. Wegener

10:00 - 10:30 **Coffee Break**

10:30 - 12:30

TRACK A (Auditorium)	TRACK C (Sala Teatro)
Session A.1 - Graph Theory **Chair: G. F. Italiano**	**C.1 - Zero Knowledge and Signatures** **Chair: A. Kiyayias**
Martin Grohe and Oleg Verbitsky *Testing Graph Isomorphism in Parallel by Playing a Game*	Ivan Visconti *Efficient Zero Knowledge on the Internet*
Amin Coja-Oghlan and Andre Lanka *The spectral gap of random graphs with given expected degrees*	Jun Furukawa, Kaoru Kurosawa and Hideki Imai *An Efficient Compiler from Sigma-Protocol to 2-move Deniable Zero-Knowledge*
Douglas Carroll, Ashish Goel and Adam Meyerson *Embedding Bounded Bandwidth Graphs into l_1*	Damien Vergnaud *New Extensions of Pairing-based Signatures into Universal Designated Verifier Signatures*
Martin Dyer, Leslie Ann Goldberg and Mike Paterson *On counting homomorphisms to directed acyclic graphs*	Rosario Gennaro and Silvio Micali *Independent Zero-Knowledge Sets*

12:30 - 14:30 **Lunch**

ICALP'06 Programme: Monday July 10, 2006 (Afternoon)

	TRACK A (Auditorium)	TRACK C (Sala Teatro)
14:30 - 16:00	**A.2 - Quantum Computing** **Chair. P. Spirakis**	**C.2 - Cryptographic protocols** **Chair: J. C. Mitchell**
	Ben Reichardt *Fault-tolerance threshold for a distance-three quantum code (Extended abstract)*	Daniele Micciancio and Saurabh Panjwani *Corrupting One vs. Corrupting Many: The Case of Broadcast and Multicast Encryption*
	Ronald de Wolf *Lower Bounds on Matrix Rigidity via a Quantum Argument*	Pedro Adao and Cedric Fournet. *Cryptographically Sound Implementations for Communicating Processes*
	Frederic Magniez, Dominic Mayers, Michele Mosca and Harold Ollivier *Self-Testing of Quantum Circuits*	Detlef Kähler, Ralf Küsters and Thomas Wilke *A Dolev-Yao-based Definition of Abuse-free Protocols*

16:00- 16:30 **Coffee Break**

16:30 - 18:00	**A.3 – Randomness** **Chair. I. Wegener**	**C.3 - Secrecy and protocol analysis** **Chair: C. Madows**
	Chia-Jung Lee, Chi-Jen Lu and Shi-Chun Tsai *Deterministic Extractors for Independent-Symbol Sources*	Rajeev Alur, Pavol Cerny and Steve Zdancewic. *Preserving Secrecy under Refinement*
	Jaikumar Radhakrishnan *Gap amplification in PCPs using lazy random walks*	Michele Boreale. *Quantifying information leakage in process calculi*
	Magnus Bordewich, Martin Dyer and Karpinski Marek *Stopping Times, Metrics and Approximate Counting*	S. Delaune, P. Lafourcade, D. Lugiez and R. Treinen *Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or*

18:00 - 18:30 **IBM Talk** **Auditorium**
Security and privacy challenges in industrial research
Birgit Pfizmann, IBM Zurich, CH
Chair: M. Bugliesi

18:30 - 20:00 **Welcome Reception**

ICALP'06 Programme: Tuesday July 11, 2006

9:00 - 10:00 **ICALP Invited Lecture** **Auditorium**
Differential Privacy
Cynthia Dwork, Microsoft Research, Silicon Valley, USA
Chair: B. Preneel

10:00 - 10:30 **Coffee Break**

	Track A (Auditorium)	Track A (Room 1E)	Track C (Sala Teatro)
10:30 - 12:30	**A.4.1 - Formal Languages** ***Chair: O. Watanabe***	**A.4.2 - Approximation Algorithms I** ***Chair: B. Monien***	**C.4 – Cryptographic primitives** ***Chair: Y. Dodis***
	Michal Kunc *Algebraic characterization of the finite power property*	Mohit Singh and R Ravi *Delegate and Conquer: An LP-based approximation algorithm for Minimum Degree MSTs*	Vadim Lyubashevsky and Daniele Micciancio. *Generalized Compact Knapsacks are Collision Resistant*
	Turlough Neary and Damien Woods *P-completeness of cellular automaton Rule 110*	Naveen Garg and Amit Kumar *Better Algorithms for Minimizing Average Flow-time on Related Machines*	Vivien Dubois, Louis Granboulan and Jacques Stern. *An Efficient Provable Distinguisher for HFE*
	Christos Kapoutsis *Small sweeping 2NFAs are not closed under complement*	Kamalika Chaudhuri, Satish Rao, Samantha Riesenfeld and Kunal Talwar *A Push-Relabel Algorithm for Approximating Degree Bounded MSTs*	Krzysztof Pietrzak. *A Tight Bound for EMAC*
	Mikolaj Bojanczyk, Mathias Samuelides, Thomas Schwentick and Luc Segoufin *On the expressive power of pebble automata*	Shuheng Zhou and Satish Rao *Edge Disjoint Paths in Moderately Connected Graphs*	Frederik Armknecht and Matthias Krause. *Constructing single- and multi-output Boolean functions with maximal immunity*

12:30 - 14:30 **Lunch**

ICALP'06 Programme: Tuesday July 11, 2006 (Afternoon)

	Track A (Auditorium)	Track A (Room 1E)	Track C (Sala Teatro)
14:30 - 16:00	**A.5.1 - Approximation Algorithms II** ***Chair: J.-Y. Cai***	**A.5.2 - Graph Algorithms I** ***Chair: F. Meyer auf der Heide***	**C.5 - Bounded storage and quantum models** ***Chair: C. Dwork***
	Leah Epstein and Asaf Levin *A robust APTAS for the classical bin packing problem*	Ramesh Hariharan, Telikepalli Kavitha and Kurt Mehlhorn *A Faster Deterministic Algorithm for Minimum Cycle Bases in Directed Graphs*	Danny Harnik and Moni Naor. *On Everlasting Security in the Hybrid Bounded Storage Model*
	Subhash Khot and Ashok Kumar Ponnuswami *Better Inapproximability Results for MaxClique, Chromatic Number and Min-3Lin-Deletion*	Virginia Vassilevska, Ryan Williams and Raphael Yuster *Finding the smallest H-subgraph in real weighted graphs and related problems*	Yevgeniy Dodis and Renato Renner. *On the Impossibility of Extracting Classical Randomness Using a Quantum Computer*
	Rolf Harren *Approximating the Orthogonal Knapsack Problem for Hypercubes*	Piotr Sankowsk *Weighted Bipartite Matching in Matrix Multiplication Time*	Akinori Kawachi and Tomoyuki Yamakami. *Quantum Hardcore Functions by Complexity-Theoretical Quantum List Decoding*

16:00 - 16:30 **Coffee Break**

16:30 - 18:00	**A.6.1 - Algorithms I** ***Chair: I. Wegener***	**A.6.2 - Complexity I** ***Chair: T. Thierauf***	**C.6 – Foundations** ***Chair: R. Gennaro***
	Irene Finocchi, Fabrizio Grandoni and Giuseppe F. Italiano *Optimal Resilient Sorting and Searching in the Presence of Memory Faults*	Arist Kojevnikov *Exponential Lower Bound on the Size of Static Lovasz-Schrijver Calculus*	Iftach Haitner, Danny Harnik and Omer Reingold. *Efficient Pseudorandom Generators from Exponentially Hard One-Way Functions*
	Kurt Mehlhorn and Ralf Osbild *Reliable and Efficient Computational Geometry via Controlled Perturbation*	Lance Fortnow, John Hitchcock, A. Pavan, N. V. Vinodchandran and Fengming Wang *Extracting Kolmogorov Complexity with Applications to Dimension Zero-One Laws*	Pierre-Alain Fouque, Jacques Stern, David Pointcheval and Sebastien Zimmer. *Hardness of Distinguishing the MSB or LSB of Secret Keys in Diffie-Hellman and Related Schemes*
	I. Caragiannis, M. Flammini, C. Kaklamanis, P. Kanellopoulos and L. Moscardelli *Tight bounds for selfish and greedy load balancing*	Parikshit Gopalan, Phokion Kolaitis, Elitza Maneva and Christos Papadimitriou *The Connectivity of Boolean Satisfiability: Computational and Structural Dichotomies*	Ricardo Corin and Jerry den Hartog. *A Probabilistic Hoare-style logic for Game-based Cryptographic Proofs*

18:80 - 19:30 **EATCS Assembly** **Auditorium**

ICALP'06 Programme: Wednesday July 12, 2006

9:00 - 10:00 **ICALP / PPDP Invited Lecture** **Auditorium**
Composable memory transactions
Simon Peyton Jones, Microsoft Research, Cambridge, UK
Chair: V. Sassone

10:00 - 10:30 **Coffee Break**

	Track A (Auditorium)	Track B (Sala Teatro)	Track C (Room 1E)
10:30 - 12:30	**A.7 - Data Structures and Linear Algebra** ***Chair: M. Krause***	**B.1 – Games** ***Chair: P. Bouyer***	**C.7 - Multi-party protocols** ***Chair: L. Granboulan***
	Richard Cole, Tsvi Kopelowitz and Moshe Lewenstein *Suffix Trays and Suffix Trists: Structures for Faster Text Indexing*	Wieslaw Zielonka and Hugo Gimbert *Deterministic priority mean-payoff games as limits of discounted games*	Duong Hieu Phan, Rei Safavi-Naini and Dongvu Tonien. *Generic Construction of Hybrid Public Key Traitor Tracing with Full-Public-Traceability*
	Alexander Golynski *Optimal lower bounds for rank and select indexes*	Kousha Etessami and Mihalis Yannakakis. *Recursive Concurrent Stochastic Games*	Douglas Wikström and Jens Groth. *An Adaptively Secure Mix-Net Without Erasures*
	A. Kaporis, C. Makris, S. Sioutas, A. Tsakalidis, K. Tsichlas and C. Zaroliagis *Dynamic Interpolation Search Revisited*	Eryk Kopczynski *Half-positional Determinacy of Infinite Games*	Tamir Tassa and Nira Dyn. *Multipartite Secret Sharing by Bivariate Interpolation*
	Gudmund Skovbjerg Frandsen and Peter Frands Frandsen *Dynamic Matrix Rank*	Colin Stirling *A game-theoretic approach to deciding higher-order matching*	Michel Abdalla, Dario Catalano, Alexander Dent, John Malone-Lee, Gregory Neven and Nigel Smart. *Identity-Based Encryption Gone Wild*

12:30 - 14:30 **Lunch**

14:30 - 20:00 **ICALP Excursion -- Murano Burano Torcello**

ICALP'06 Programme: Thursday July 13, 2006

9:00 - 10:00 **ICALP Invited Lecture** **Auditorium**

The One Way to Quantum Computation

Prakash Panangaden, Mc Gill University, Canada

Chair: V. Sassone

10:00 - 10:30 **Coffee Break**

10:30 - 12:30

Track A (Auditorium)	Track A (Room 1E)	Track B (Sala Teatro)
A.8.1 - Graphs	**A.8.2 - Complexity II**	**B.2 - Semantics**
Chair: T. Roughgarden	***Chair: O. Watanabe***	***Chair: M. Dezani-Ciancaglini***
Xin He and Huaming Zhang *Nearly Optimal Visibility Representations of Plane Graphs*	Thomas Thierauf, Minh Thanh Hoang and Meena Mahajan *On the unique bipartite perfect matching Problem*	Kohei Honda, Martin Berger and Nobuko Yoshida *Descriptive and Relative Completeness of Logics for Higher-Order Functions*
Hristo Djidjev and Imrich Vrt'o *Planar Crossing Numbers of Genus g Graphs*	John Hitchcock and A. Pavan *Comparing Reductions to NP-Complete Sets*	Paul Blain Levy *Jumbo Lambda Calculus*
Toshihiro Fujito *How to trim an MST: A 2-approximation algorithm for minimum cost tree cover*	Deeparnab Chakrabarty, Aranyak Mehta and Vijay Vazirani *Towards a Theory of Intelligent Design or Design as Easy as Optimization*	Esfandiar Haghverdi *Typed GoI for Exponentials*
Guy Kortsarz and Zeev Nutov *Tight Approximation Algorithm for Connectivity Augmentation Problems*	Xi Chen and Xiaotie Deng *On the Complexity of 2D Discrete Fixed Point Problem*	Stefano Guerrini and Patrizia Marzuoli *Commutative Locative Quantifiers for Multiplicative Linear Logic*

12:30 - 14:30 **Lunch**

ICALP'06 Programme: Thursday July 13, 2006 (Afternoon)

14:30 - 16:00

Track A (Auditorium)	Track A (Room 1E)	Track B (Sala Teatro)
A.9.1 - Game Theory I	**A.9.2 - Algorithms**	**B.3- Automata I**
Chair: T. Roughgarden	***Chair: F. Meyer auf der Heide***	***Chair: J. Karhumaki***
Burkhard Monien, Martin Gairing and Karsten Tiemann *Routing (Un-) Splittable Flow in Games with Player-Specific Linear Latency Functions*	David Doty, Jack Lutz and Satyadev Nandakumar *Finite-State Dimension and Real Arithmetic*	Filip Murlak *The Wadge Hierarchy of Deterministic Tree Languages*
Constantinos Daskalakis, Alex Fabrikant and Christos H. Papadimitriou *The Game World is Flat: The Complexity of Nash Equilibria in Succinct Games*	Thore Husfeldt and Andreas Björklund *Exact Algorithms for Exact Satisfiability and Number of Perfect Matchings*	Patricia Bouyer, Serge Haddad and Pierre-Alain Reynier *Timed Petri Nets and Timed Automata: On the Discriminating Power of Zeno Sequences*
Roberto Cominetti, Jose R. Correa and Nicolas E. Stier-Moses *Network Games with Atomic Players*	Paolo Ferragina, Giovanni Manzini and Raffaele Giancarlo *The Myriad Virtues of Wavelet Trees*	Tomasz Jurdzinski *On Complexity of Grammars Related to the Safety Problem*

16:00 - 16:30 **Coffee Break**

16:30 - 18:00 **Goedel Award Ceremony** **Auditorium**

20:00 - 23:00 **ICALP Banquet**

ICALP'06 Programme: Friday July 14, 2006

	Track A (Auditorium)	Track B (Sala Teatro)
9:00 - 10:30	**A.10 - Game Theory II** ***Chair: T. Roughgarden***	**B.4 - Models** ***Chair: R. Amadio***
	Dimitris Fotakis, Spyros Kontogiannis and Paul Spirakis *Atomic Congestion Games among Coalitions*	Rasmus Ejlers Møgelberg *Interpreting Polymorphic FPC into domain theoretic models of parametric polymorphism*
	Kasturi Varadarajan, Bruno Codenotti and Luis Rademacher *Computing Equilibrium Prices in Exchange Economies with Tax Distortions*	Radha Jagadeesan, Alan Jeffrey, Corin Pitcher and James Riely. *LRBAC: Programming With Role-Based Access Contro*
	V. Auletta, R. De Prisco, P. Penna, G. Persiano and C. Ventre *New Constructions of Mechanisms with Verification*	Juhani Karhumaki, Michal Kunc and Alexander Okhotin *Communication of two stacks and rewriting*
10:30 - 11:00	**Coffee Break**	
11:00 - 13:00	**A.11 - Networks, Circuits and Regular Expressions** ***Chair: A. Gál***	**B.5 - Equations** ***Chair: C. Palamidessi***
	A. Fiat, H. Kaplan., M.Levy, S. Olonetsky and R. Shabo *On the Price of Stability for Designing Undirected Networks with Fair Cost Allocations*	Luca Aceto, Taolue Chen, Wan Fokkink and Anna Ingolfsdottir *On the Axiomatizability of Priority*
	Amos Korman and David Peleg *Dynamic Routing Schemes for General Graphs*	Luca Aceto, Wan Fokkink, Anna Ingolfsdottir and Bas Luttik *A finite equational base for CCS with left merge and communication merge*
	Kei Uchizawa, Rodney Douglas and Wolfgang Maass *Energy Complexity and Entropy of Threshold Circuits*	Markus Lohrey and Géraud Sénizergues *Theories of HNN-extensions and amalgamated products*
	Philip Bille *New Algorithms for Regular Expression Matching*	Wong Karianto, Aloys Krieg and Wolfgang Thomas *On Intersection Problems for Polynomially Generated Sets*
13:00 - 14:30	**Lunch**	

ICALP'06 Programme: Friday July 14, 2006 (Afternoon)

	Track A (Auditorium)	Track B (Sala Teatro)
14:30 - 16:00	**A.12 - Fixed Parameter Complexity and Approximation Algorithms** **Chair: B. Monien**	**B.6 – Logics** **Chair: M. Nielsen**
	Dániel Marx *A Parameterized View on Matroid Optimization Problems*	Ittai Balaban, Amir Pnueli and Lenore Zuck. *Invisible Safety of Distributed Protocols*
	G. Blelloch, K. Dhamdhere, E. Halperin, R. Ravi, R. Schwartz and S. Sridhar *Fixed Parameter tractability of Binary Near-Perfect Phylogenetic Tree Reconstruction*	Piero A. Bonatti, Carsten Lutz, Aniello Murano and Moshe Y. Vardi *The Complexity of Enriched mu-Calculi*
	G. Baier, T. Erlebach, A. Hall, E. Koehler, H. Schilling and M. Skutella *Length-Bounded Cuts and Flows*	Michael Benedikt and Christoph Koch *Interpreting Tree-to-Tree Queries*
16:00 - 16:30	**Coffee Break**	
16:30 - 18:00	**A.13 - Graph Algorithms** ***Chair: M. Krause***	**B.7 - Automata II** ***Chair: J.-E. Pin***
	Amin Coja-Oghlan *An adaptive spectral heuristic for partitioning random graphs*	Blaise Genest and Anca Muscholl *Constructing Exponential-size Deterministic Zielonka Automata*
	Jin-Yi Cai and Vinay Choudhary *Some Results on Matchgates and Holographic Algorithms*	Marius Bozga Radu Iosif and Yassine Lakhnech *Flat Parametric Counter Automata*
	Julian Mestre *Weighted Popular Matchings*	Qiqi Yan *Lower Bounds for Complementation of omega-Automata via the Full Automata Technique*
18.00	**ICALP'06 Closing**	

Third Workshop on Constraint Handling Rules
CHR 2006 - July 9 2006 ROOM R2

9.15	**Opening**
9:30 - 10:00	**Session 1**
	Edmund S. L. Lam, Martin Sulzmann *Representing Linear-Logic Agents in CHR*
10:00 - 10:30	**Coffee Break**
10:30 - 11:30	**Invited Lecture** *LMNtal as a Unifying Declarative Language* **Kazunori Ueda, Waseda University, Japan**
11:30 - 12:30	**Session 2**
	Martin Kaeser, Marc Meister *Implementation of an F-Logic Kernel in CHR*
	Thom Frühwirth *Deriving Linear-Time Algorithms from Union-Find in CHR*
12:30 - 14:30	**Lunch**
14:30 - 16:00	**Session 3**
	Gregory J. Duck, Peter J. Stuckey, Martin Sulzmann *Observable Confluence for Constraint Handling Rules*
	Marc Meister, Thom Frühwirth *Complexity of the CHR Rational Tree Equation Solver*
	Maurizio Gabbrielli, Maria Chaira Meo, Paolo Tacchella *A Compositional Semantics for CHR with Propagation Rules*
16:00- 16:30	**Coffee Break**
16:30 - 18:00	**Session 4**
	Leslie De Koninck, Tom Schrijvers, Bart Demoen *Search Strategies in CHR(Prolog)*
	Peter Van Weert, Jon Sneyers, Tom Schrijvers, Bart Demoen *Constraint Handling Rules with Negations as Absence*
	Tom Schrijvers, Neng-Fa Zhou, Bart Demoen \ *Translating Constraint Handling Rules into Action Rules*
18.00	**Discussion and Closing**

Formal and Computational Cryptography
FCC 2006 - July 9, 2006 ROOM 9A

8.50	**Opening**
9:00 - 10:00	**Session 1: Computationally sound proofs (chair: Ralf Küsters)**
	Michael Backes and Peeter Laud. *Computationally Sound Secrecy Proofs by Mechanized Flow Analysis.*
	Anupam Datta, Ante Derek, John Mitchell, Arnab Roy, Vitaly Shmatikov, Mathieu Turuani and Bogdan Warinschi. *Computationally Sound Compositional Logic for Security Protocols.*
10:00 - 10:30	**Coffee Break**
10:30 - 12:30	**Session 2: (Un)Sound abstractions (chair: Ran Canetti)**
	Pedro Adao and Cédric Fournet. *Language Design for Computationally Sound Communications Abstractions*
	Yassine Lakhnech, Laurent Mazare and Bogdan Warinschi *Soundness of Symbolic Equivalence for Modular Exponentiation.*
	Flavio D. Garcia and Peter van Rossum. *Sound and Complete Computational Interpretation of Symbolic Hashes in the Standard Model.*
	Michael Backes, Birgit Pfitzmann and Michael Waidner *Soundness Limits of Dolev-Yao Models.*
12:30 - 14:30	**Lunch**
14:30 - 16:00	**Session 3: Cryptographic Models (chair: Joshua Guttman)**
	Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira and Roberto Segala. *Using Task-Structured Probabilistic I/O Automata to Analyze Cryptographic Protocols.*
	Michael Backes, Anupam Datta, Ante Derek, John Mitchell, Ajith Ramanathan and Andre Scedrov *Games and the Impossibility of Realizable Ideal Functionality*
	Suzana Andova, Kristian Gjøsteen, Lillian Kråkmo, Stig Frode Mjølsnes and Saša Radomirović. *An example of proving UC-realization with formal methods.*
16:00- 16:30	**Coffee Break**
16:30 - 17:30	**Business Meeting**

Membrane Computing and Biologically Inspired Process Calculi
MeCBIC - July 9, 2006 ROOM 9B

8.50 **Opening**

9:00 - 10:00 **Invited Lecture**
Title TBA
Luca Cardelli, Microsoft Research, Cambridge, UK

10:00 - 10:30 **Coffee Break**

10:30 - 11:30 **Session 1**

Robert Brijder, Matteo Cavaliere, Agustin Riscos-Nunez, Grzegorz Rozenberg, Dragos Sburlan
Membrane Systems with Marked Membranes

Matteo Cavaliere, Sean Sedwards
Membrane Systems with Peripheral Proteins: Transport and Evolution

Daniel Diaz-Pernil, Miguel A. Gutirrez-Naranjo, Mario J. Perez-Jimenez, Agustin Riscos-Nunez
An Efficient Solution to 3-COL with tissue P Systems

11:30 - 12:30 **Session 2**

Giorgio Delzanno, Roberto Montagna
On Reachability and Spatial Reachability in Fragments of BioAmbients

Cosimo Laneve, Fabien Tarissan
A simple calculus for proteins and cells

Federica Ciocchetta, Corrado Priami
Biological transactions for quantitative models

Cristian Versari
Encoding Catalytic P Systems in Pi@

MeCBIC - July 9, 2006 (Afternoon) ROOM 9B

12:30 - 14:30 **Lunch**

14:30 - 15:30 **Invited Lecture**
Title TBA
Geroge Paun, Institute of Mathematics of the Romanian Academy, RO

15:30 - 16:00 **Session 3**

Giuditta Franco, Maurice Margenstern
Universal Computations by Floating Strings

Verena Wolf
Modeling of Biochemical Reactions by Stochastic Automata Networks

16:00- 16:30 **Coffee Break**

16:30 - 18:00 **Session 4**

Julian Gutierrez, Jorge A. Perez, Camilo Rueda, Frank D. Valencia
A Timed Process Calculus for Modeling and Verifying Biological Systems

Antonio Vitale, Giancarlo Mauri
Communication via mobile vesicles in Brane Calculi

Corrado Priami, Alessandro Romanel
The Decidability of the Structural Congruence for Beta-binders

Rudolf Freund, Marion Oswald
Tissue P Systems with Mate and Drip Operations

B. Aman, G. Ciobanu
Translating Mobile Ambients into P Systems

Xian Xu, Xiaoju Dong, Yuxi Fu
A Model in k for DNA Addition

18.00 **Closing**

International Workshop on Algorithmic Aspects of Wireless Sensor Networks
ALGOSENSORS - July 15, 2006 ROOM 1E

8.30	**Opening**
8:40 - 9:40	**Invited Lecture** *Computation, Timing and Control in Sensor Networks* **P.R. Kumar (University of Illinois, Urbana-Champaign, USA**
9:40 - 10:00	**Session 1 - chair: Sotiris Nikoletseas**
	Paola Flocchini; Giuseppe Prencipe; Nicola Santoro *Self-Deployment Algorithms for Mobile Sensors*
10:00 - 10:30	**Coffee Break**
10:30 - 12:30	**Session 2 - chair: Jose Rolim**
	Alan Albert Bertossi; Stephan Olariu; Cristina M. Pinotti *Efficient Training of Sensor Networks*
	Davide Bilo; Guido Proietti *On the Complexity of Minimizing Interference in Ad-Hoc and Sensor Networks*
	Ludek Kucera; Stepan Kucera *Wireless Communication in Random Geometric Topologies*
	Volker Turau *Computing Bridges, Articulations, and 2-Connected Components in Wireless Sensor Networks*
	Azzedine Boukerche; Regina Araujo *Context Interpretation Based Wireless Sensor Networks for the Emergency Preparedness Class of Applications*
	Iyad Kanj; Ljubomir Perkovic *Improved Stretch Factor for Bounded-Degree Planar Power Spanners of Wireless Ad-Hoc Networks*
12:30 - 14:30	**Lunch**

ALGOSENSORS - July 15, 2006 (Afternoon) ROOM 1E

14:30 - 16:00	**Session 3 - Chair: Pekka Orponen**
	Vasia Liagkou; Effie Makri; Paul Spirakis; Yannis Stamatiou *The Threshold Behaviour of the Fixed Radius Random Graph Model and Applications to the Key Management Problem of Sensor Networks*
	Tassos Dimitriou *Securing Communication Trees in Sensor Networks*
	Marcin Zawada; Jacek Cichon; Mirek Kutylowski *Adaptive Initialization Algorithm for Ad Hoc Radio Networks with Carrier Sensing*
	Pierre Leone; Luminita Moraru; Olivier Powell; Jose Rolim *A Localization Algorithm for Wireless Ad-hoc Sensor Networks with Traffic Overhead Minimization by Emission Inhibition*
	Zsolt Fekete; Tibor Jordan *Uniquely Localizable Networks with Few Anchors*
16:00- 16:30	**Coffee Break**
16:30 - 18:00	**Session 4 - Chair: Jan van Leeuwen**
	Magnus Halldorsson; Takeshi Tokuyama *Minimizing Interference of a Wireless Ad-Hoc Network in a Plane*
	Sandip Roy; Yan Wan; Ali Saberi *A Flexible Algorithm for Sensor Network Partitioning and Self-Partitioning Problems*
	Colette Johnen; Nguyen Huy *Self-Stabilizing Weight-Based Clustering Algorithm for Ad hoc sensor Networks*
	Ivan Stojmenovic; Amiya Nayak; Francisco Ovalle-Martinez *Area Based Beaconless Reliable Broadcasting in Sensor Networks*
	Chalermek Intanagonwiwat *Declarative Resource Naming for Macroprogramming Wireless Networks of Embedded Systems*
18.00	**Closing**

Classical Logic and Computation
CL&c - July 15, 2006 ROOM 2

9.00	**Opening**
9:00 - 10:00	**Invited Lecture** *Investigations into the Duality of Computation* **Hugo Herbelin**
10:00 - 10:30	**Coffee Break**
10:30 - 11:30	**Session 1**
	Stéphane Lengrand and Alexandre Mique *A classical version of system Fω*
	Kentaro Kikuchi *Call-by-Name Reduction and Cut-Elimination on Classical Logic*
	Stefano Berardi and Yoriyuki Yamagata *A sequent calculus for Limit Computable Mathematics*
12:30 - 14:30	**Lunch**
14:30 - 15:30	**Invited Lecture** *Programs from Classical Proofs in Minlog* **Monika Seisenberger**
15:30 - 16:00	**Session 2**
	Christian Urban and Diana Ratiu Classical Logic is better than Intuitionistic Logic: A Conjecture about Double-Negation Translations
16:00 - 16:30	**Coffee Break**
16:30 - 17:45	**Session 3**
	Lutz Straßburger *What could a Boolean category be?*
	Silvia Likavec and Pierre Lescanne *On untyped Curien-Herbelin calculus*
	Robert K. Meyer *Types, Relevance & Classical Logic*
17.45	**Closing**

1st Int. Workshop on Security and Rewriting Techniques
SecReT 2006 - July 15, 2006 ROOM 9A

8.50	**Opening**
9:00 - 10:00	**Invited Lecture** *Deciding Protocol Insecurity with Rewriting Techniques* **Michael Rusinowitch**
10:00 - 10:30	**Coffee Break**
10:30 - 11:30	**Session 1**
	T. Hardin, M. Jaume, C. Morisset *Access control and rewrite systems*
	A. Santana de Oliveira *Rewriting-based access control policies*
	T. Chothia, D. Duggan, Y. Wu *An End-to-End Approach to Distributed Policy Language Implementation*
	P. Lafourcade *Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption*
12:30 - 14:30	**Lunch**
14:30 - 16:00	**Session 2**
	S. Escobar, C. Meadows, J. Meseguer *Equational Cryptographic Reasoning in the Maude-NRL Protocol Analyzer*
	M. Nesi *Specification and Analysis of security Protocols by Rewriting*
	A. Bouhoula, F. Jacquemard *Security Protocols Verification with Implicit Induction and Explicit Destructors*
16:00- 16:30	**Coffee Break**
16:30 - 17:00	**Session 3**
	V. Vasconcelos, N. Yoshida *Language primitives and type discipline for structured communication-based programming revisited*
17:00 - 17:30	**Discussion and future SecReT directions**
TBA	**Workshop Dinner**

2nd International Workshop on Developments in Computational Models
DCM 2006 - July 16, 2006 ROOM 2

9.00 **Opening**

9:00 - 10:00 **Invited Lecture**
Every computable function is linear (in a sense)
Maribel Fernández

10:00 - 10:30 **Coffee Break**

10:30 - 11:30

Session 1
Marco Carbone, Kohei Honda and Nobuko Yoshida *A Calculus of Global Interaction based on Session Types*
Simon Gay, Rajagopal Nagarajan and Nikolaos Papanikolaou *Probabilistic Model-Checking of Quantum Protocols*
Michel Cosnard and Luigi Liquori *Virtual Organizations in Arigatoni: the formal model*

12:30 - 14:30 **Lunch**

14:30 - 16:00

Session 2
Nikolaos Siafakas A fully labelled lambda calculus: Towards closed reduction in the Geometry of Interaction Machine
Germain Faure *Term collections in lambda and rho-calculi*
Mircea-Dan Hernes *Light Dialectica Extraction from a Classical Fibonacci Proof*
Robert K. Meyer *Types, Relevance & Classical Logic*

16:00 - 16:30 **Coffee Break**

16:30 - 18:00

Session 3
Luca Fossati *Handshake Games*
Jayshan Raghunandan and Alexander J. Summers *On the Computational Representation of Classical Logical Connectives*
Bob Meyer *Better Bubbling*

18.00 **Closing**

Improving Exponential Time Algorithms
iETA - July 16, 2006 ROOM 1E

8.50 **Opening**

9:00 - 10:00

Session 1
Tobias Riege and Joerg Rothe (Heinrich-Heine-Univ. Duesseldorf) *Improving exponential-time algorithms for NP-complete problems* ***(Tutorial)***
Tobias Riege, Joerg Rothe, Holger Spakowski (Heinrich-Heine-Univ. Duesseldorf) and Masaki Yamamoto (Kyoto Univ.) *An improved exact algorithm for the domatic number problem*

10:00 - 10:30 **Coffee Break**

10:30 - 12:30

Session 2
Andreas Bjoerklund and Thore Husfeldt (Lund Univ.) *Inclusion-exclusion algorithms for counting set partitions*
Heidi Gebauer (ETH) and Yoshio Okamoto (Toyohashi Univ. of Tech.) *Fast exponential-time algorithms for the forest counting in graph classes*
Takehiro Ito (Tohoku Univ.), Yoshio Okamoto (Toyohashi Univ. of Tech.), and Takeshi Tokuyama (Tohoku Univ.) *Algorithms for the full Steiner tree problem*
Dieter Kratsch (Univ. Paul Verlaine - Metz) *Lower bounds on exponential time algorithms* ***(Tutorial)***

12:30 - 14:30 **Lunch**

14:30 - 16:00 **Session 3**

Fedor V. Fomin (Univ. of Bergen)
Treewidth and exact algorithms

Federico Della Croce (Politecnico di Torino), Marcin Kaminski (Rutgers Univ.), and Vangelis Paschos (Univ. Paris-Dauphine)
An exact algorithm for solving Max-Cut on graphs with bounded maximum degree

Kazuo Iwama and Takuya Nakashima (Kyoto Univ.)
TSP for degree-restricted graphs

16:00- 16:30 **Coffee Break**

16:30 - 17:45 **Session 3**

Falk Hueffner, Rolf Niedermeier, and S. Wernicke (Friedrich-Schiller-Univ. Jena)
Techniques for practical fixed-parameter algorithms ***(Tutorial)***

Magnus M. Halldorsson (Univ. of Iceland), Takeshi Tokuyama (Tohoku Univ.), and Alexander Wolff (Univ. Karlsruhe)
Improved fixed-parameter algorithms for non-crossing subgraphs

17:45 - 18:00 **Discussion**

2nd Workshop on Cryptography for Ad Hoc Networks
WCAN 2006 - July 16 2006 ROOM 9A

8.50 **Opening**

9:00 - 10:00 **Invited Lecture**
Algorithmic Techniques for Maintaining Shortest Routes in Dynamic Networks
C. Demetrescu and G. Italiano, Universita` di Roma "La Sapienza", Italy

10:00 - 10:30 **Coffee Break**

10:30 - 11:30 **Session 1: Key Distribution**

Ioannis Chatzigiannakis (CTI and University of Patras, Greece)
Elisavet Konstantinou (University of the Aegean, Greece)
Vasiliki Liagkou and Paul Spirakis (CTI and University of Patras, Greece)
Design, Analysis and Performance Evaluation of Group Key Establishment in Wireless Sensor Networks

V. Daza (Universitat Rovira i Virgili, Spain),
P. Morillo and C. Rafols (Universitat Politecnica de Catalunya, Spain)
On Dynamic Distribution of Private Keys over MANETs,

11:30 - 12:30 **Session 2: Secure Routing**

A. M. Hegland, P. Spilling, L. Nilsen (University of Oslo, Norway), and Ø. Kure (Norwegian University of Science and Technology, Norway)
Hybrid Protection of OLSR

G. Di Crescenzo (Telcordia Technologies, USA)
Secure Node Discovery over Ad Hoc Networks and Applications,

12:30 - 14:30 **Lunch**

WCAN 2006 - July 16 2006 (Afternoon) ROOM 9A

14:30 - 16:00	**Session 3: Encryption**
	R. Curtmola and S. Kamara (The Johns Hopkins University, USA) *A Mechanism for Communication-Efficient Broadcast Encryption over Wireless Ad Hoc Networks*
	A. Vitaletti and G. Palombizio (Universita' di Roma ``La Sapienza'', Italy) *Rijndael for sensor networks: is speed the main issue?*
	M. Yoshida and T. Fujiwara (Osaka University, Japan) *On the Security of Tag-KEM for Signcryption (work in progress)*
16:00- 16:30	**Coffee Break**
16:30 - 18:00	**Session 4 - Threshold Cryptography**
	R. Di Pietro, L. Mancini and G. Zanin (Universita' di Roma ``La Sapienza'', Italy) *Efficient and Adaptive Threshold Signatures for Ad Hoc Networks*
	W. Bagga, S. Crosta, P. Michiardi, and R. Molva (Institut Eurecom, France) *Establishment of Ad-Hoc Communities through Policy-Based Cryptography (work in progress)*
	J. Li and Y. Wang (Sun Yat-sen University, P.R. China) *Threshold Identity Based Encryption Scheme without Random Oracle (work in progress)*
18.00	**Closing**

UNIVERSITÀ CA' FOSCARI VENEZIA

DIPARTIMENTO DI INFORMATICA

VENICE INTERNATIONAL UNIVERSITY

Microsoft Research

IBM

VENIS

VENEZIA RICERCHE

Conference Secretariat

key congress & communication

Via Makallè, 75. I 35138 Padova, Italy
Tel. ++39 049 8729511 fax ++39 049 8729512 e-mail: info@keycongress.com