ICALP 2008 Programme

Monday, July 7th

	Track A (a)	Track A (b)	Track B	Track C
	Algorithms, Automata, Complexity and Games		*Logic, Semantics, and Theory of Programming*	*Security and Cryptography Foundations*
08:50 – 09:00	***Opening and Welcome***			
09:00 – 10:00	**Invited talk: S. Muthu Muthukrishnan, Google, USA** ***Internet Ad Auctions: Insights and Directions*** Chair: Magnus M. Halldorsson			
10:00 – 10:30	*Coffee break*			
10:30 – 12:30	**Complexity: Boolean functions and circuits** Chair: Leslie Ann Goldberg Buchfuhrer, Umans: *The complexity of Boolean formula minimization* Glasner, Lee, Malkin, Servedio, Wan, Wee: *Optimal Cryptographic Hardness of Learning Monotone Functions* Boros, Elbassioni, Makino: *On Berge Multiplication for Monotone Boolean Dualization* Saxena: *Diagonal Circuit Identity Testing and Lower Bounds*	**Data structures** Chair: Pino Italiano Yin: *Cell-Probe Proofs and Nondeterministic Cell-Probe Complexity* Milan Ruzic: *Constructing Efficient Dictionaries in Close to Sorting Time* Albers,Lauer: *On List Update with Locality of Reference* Blelloch, Vassilevska, Williams: *A New Combinatorial Approach For Sparse Graph Problems*	Track B starts after lunch	**Theory** Chair: Jesper Buus Nielsen Pietrzak, Sjödin: *Weak Pseudorandom Functions in Minicrypt* Altmann, Jager, Rupp: *On Black-Box Ring Extraction and Integer Factorization* Canetti, Dakdouk: *Extractable Perfectly One-way Functions* Przydatek, Wullschleger: *Error-Tolerant Combiners for Oblivious Primitives*
12:30 – 14:00	*Lunch*			
14:00 – 16:00	**Random walks and random structures** Chair: Martin Dietzfelbinger Avin, Koucky, Lotker: *How to Explore a Fast-Changing World* Chaintreau, Fraigniaud, Lebhar: *Networks become navigable as nodes move and forget* Pritchard: *Fast Distributed Computation of Cuts via Random Circulations* Chebolu, Frieze, Melsted: *Finding a Maximum Matching in a Sparse Random Graph in O(n) Expected Time*	**Design and analysis of algorithms** Chair: Christos Kaklamanis Cicalese, Laber: *Function Evaluation via Linear Programming in the Priced Information Model* Azar, Birnbaum, Karlin, Mathieu, Nguyen: *Improved Approximation Algorithms for Budgeted Allocations* Bjorklund, Husfeldt, Kaski, Koivisto: *The Travelling Salesman Problem in Bounded Degree Graphs* Fomin, Villanger: *Treewidth computation and extremal combinatorics*	**Bounds** Chair: Igor Walukiewicz Björklund, Martens: *The Tractability Frontier for NFA Minimization* Gruber, Holzer: *Finite Automata, Digraph Connectivity, and Regular Expression Size* Jurdzinski: *Leftist Grammars are Nonprimitive Recursive* Jez, Okhotin: *On the computational completeness of equations over sets of natural numbers*	**Secure Computation** Chair: Ivan Visconti Hirt, Nielsen, Przydatek: *Asynchronous Multi-Party Computation With Quadratic Communication* Kolesnikov, Schneider: *Improved Garbled Circuit: Free XOR Gates and Applications* Katz, Koo, Kumaresan: *Improving the Round Complexity for VSS in Point-to-Point Networks* Canetti, Eiger, Goldwasser, Lim: *How to Protect Yourself without Perfect Shredding*
16:00 – 16:30	*Coffee break*			
16:30 – 18:00	**Scheduling** Chair: Jan van Leeuwen Plaxton: *Fast Scheduling of Weighted Unit Jobs with Release Times and Deadlines* Jansen, Thöle: *Approximation Algorithms for Scheduling Parallel Jobs: Breaking the Approximation Ratio of 2* Eisenbrand, Rothvoss: *A Bi-Criteria PTAS for Real-Time Scheduling with Fixed Priorities*	**Codes and coding** Chair: Zvi Lotker Alon, Hod: *Optimal Monotone Encodings* Iwama, Nishimura, Paterson, Raymond, Yamashita: *Polynomial-Time Construction of Linear Network Coding* Cheng, Wan: *Complexity of Decoding Positive-Rate Reed-Solomon Codes*	**Distributed computation** Chair: Roberto Amadio Neubauer, Thiemann: *Placement Inference for a Client-Server Calculus* Johansson, Parrow, Victor, Bengtson: *Extended pi-Calculi* Berger, Honda, Yoshida: *Completeness and Logical Full Abstraction in Modal Logics for Typed Mobile Processes*	**Two-party protocols and Zero-Knowledge** Chair: Krzysztof Piertrzak Kurosawa, Furukawa: *Universally Composable Undeniable Signature* Kalai, Raz: *Interactive PCP* Ostrovsky, Persiano, Visconti: *Constant-Round Concurrent Non-Malleable Zero Knowledge in the Bare Public-Key Model*
18:00 – 19:30	***Welcome reception***			

All rooms are at Reykjavik University's main building at **Ofanleiti 2, 103 Reykjavik**
Further information and corrections on conference webpage: **http://www.ru.is/icalp08/**
Conference chairs: (+354) 845 6003 (Luca), (+354) 846 7919 (Anna), (+354) 825 6384 (Magnús)

Rooms 131 a & b
Room 231 a
Room 101
Room 201

ICALP 2008 Programme

Tuesday, July 8th

	Track A *Algorithms, Automata, Complexity and Games* *(a)*	*(b)*	Track B *Logic, Semantics, and Theory of Programming*	Track C *Security and Cryptography Foundations*
09:00 – 10:00	**Invited talk: Ran Canetti, IBM T.J. Watson Research Center and MIT, USA** ***Composable Formal Security Analysis: Juggling Soundness, Simplicity and Efficiency*** Chair: Ivan Damgård			
10:00 – 10:30	*Coffee break*			
10:30 – 12:30	**Colouring** Chair: Peter Winkler Fiala, Golovach, Kratochvil: *Computational complexity of the distance constrained labeling problem for trees* Pemmaraju, Srinivasan: *The Randomized Coloring Procedure with Symmetry-Breaking* Chierichetti, Vattani: *The local nature of list colorings for graphs of high girth* Kawarabayashi: *Approximating list-coloring on a fixed surface*	**Randomness in computation** Chair: Friedhelm Meyer auf der Heide Blaeser, Hardt, Steurer: *Asymptotically Optimal Hitting Sets Against Polynomials* Andoni, Krauthgamer: *The Smoothed Complexity of Edit Distance* Kao, Schweller: *Randomized Self-Assembly for Approximate Shapes* Dietzfelbinger, Pagh: *Succinct Data Structures for Retrieval and Approximate Membership*	**Real-time and probabilistic systems** Chair: Jean-Francois Raskin Boigelot, Brusten, Bruyere: *On the Sets of Real Numbers Recognized by Finite Automata in Multiple Bases* Bouyer, Markey, Ouaknine, Worrell: *On Expressiveness and Complexity in Real-time Model Checking* Vladimerou, Prabhakar, Viswanathan, Dullerud: *STORMED hybrid systems* Brazdil, Forejt, Kucera: *Controller Synthesis and Verification for Markov Decision Processes with Qualitative Branching Time Objectives*	**Encryption with special properties/Quantum Cryptography** Chairs: Ran Canetti/Ivan Damgård Shi, Waters: *Delegating Capabilities in Predicate Encryption Systems* Goyal, Jain, Pandey, Sahai: *Bounded Ciphertext-Policy Attribute based Encryption* Hallgren, Kolla, Sen, Zhang: *Making classical honest verifier zero knowledge protocols secure against quantum attacks* Wehner, Wullschleger: *Composable Security in the Bounded-Quantum-Storage Model*
12:30 – 14:00	*Lunch*			
14:00 – 16:00	**Online and dynamic algorithms** Chair: Pino Italiano Dimitrov, Plaxton: *Competitive Weighted Matching in Transversal Matroids* Bansal, Chan, Lam, Lee: *Scheduling for Speed Bounded Processors* Haeupler, Kavitha, Mathew, Sen, Tarjan: *Faster Algorithms for Incremental Topological Ordering* Frandsen, Sankowski: *Dynamic Normal Forms and Dynamic Characteristic Polynomial*	**Approximation algorithms** Chair: Christos Kaklamanis Phillips: *Algorithms for epsilon-approximations of Terrains* Laber, Molinaro: *An Approximation Algorithm for Binary Searching in Trees* Chekuri, Khanna: *Algorithms for 2-Route Cut Problems* Borradaile, Klein: *The two-edge connectivity survivable network problem in planar graphs*	**Logic and complexity** Chair: Erich Graedel Dawar, Kreutzer: *On Datalog vs. LFP* Egri, Larose, Tesson: *Directed ST-Connectivity is not Expressible in Symmetric Datalog* Bodirsky, Grohe: *Non-dichotomies in Constraint Satisfaction Complexity* Chen: *Quantified Constraint Satisfaction and the Polynomially Generated Powers Property*	**Various Types of Hashing** Chair: Martijn Stam Hoch, Shamir: *On the Strength of the Concatenated Hash Combiner when All the Hash Functions are Weak* Naor, Segev, Wieder: *History-Independent Cuckoo Hashing* Shrimpton, Stam: *Building a Collision-Resistant Compression Function from Non-Compressing Primitives* Fischlin, Lehmann, Pietrzak: *Robust Multi-Property Preserving Combiners for Hash Functions Revisited*
16:00 – 16:30	*Coffee break, sponsored by Computer Science Review, a new Elsevier journal*			
16:30 – 18:00	***Masterclass on mathematical puzzles*** **by Peter Winkler** Apart from being a noted research mathematician, Peter Winkler is well known as a mathematical puzzles expert. He is the author of the books "*Mathematical Puzzles: A Connoisseur's Collection*" (2004) and "*Mathematical Mind-Benders*" (2007). Both books have been published by A K Peters Ltd, and have rapidly become classics on mathematical puzzles.			
18:00 – 19:30	***EATCS General Assembly*** The best paper awards and the best student paper awards for the three tracks of the ICALP 2008 conference will be made as part of the General Assembly.			

All rooms are at Reykjavik University's main building at **Ofanleiti 2, 103 Reykjavik**
Further information and corrections on conference webpage: **http://www.ru.is/icalp08/**
Conference chairs: (+354) 845 6003 (Luca), (+354) 846 7919 (Anna), (+354) 825 6384 (Magnús)

Rooms 131 a & b
Room 231 a
Room 101
Room 201

ICALP 2008 Programme

Wednesday, July 9th

	Track A		Track B	Track C
	Algorithms, Automata, Complexity and Games		*Logic, Semantics, and Theory of Programming*	*Security and Cryptography Foundations*
	(a)	*(b)*		

09:00 – 10:00

Invited talk: Bruno Courcelle, Labri, Universitè Bordeaux, France

Graph Structure and Monadic Second-order Logic: Language Theoretical Aspects

Chair: Mogens Nielsen

10:00 – 10:30 — *Coffee break*

10:30 – 12:30

Property testing

Chair: Peter Bro Miltersen

Diakonikolas, Lee, Matulef, Servedio, Wan: *Efficiently Testing Sparse GF(2) Polynomials*

Onak: *Testing Properties of Sets of Points in Metric Spaces*

Kale, Seshadhri: *An expansion tester for bounded degree graphs*

Yoshida, Ito: *Property Testing on k-Vertex-Connectivity of Graphs*

Parameterized algorithms and complexity

Chair: Giorgio Ausiello

Razgon, O'Sullivan: *Almost 2-SAT is Fixed-Parameter Tractable (Extended Abstract)*

Bodlaender, Downey, Fellows, Hermelin: *On Problems Without Polynomial Kernels (Extended Abstract)*

Koutis: *Faster algebraic algorithms for path and packing problems*

Chen, Thurley, Weyer: *Understanding the Complexity of Induced Subgraph Isomorphisms*

Words and trees

Chair: Anuj Dawar

Gomez, Guaiana, Pin: *When does partial commutative closure preserve regularity?*

Mathissen: *Weighted Logics for Nested Words and Algebraic Formal Power Series*

Bojanczyk, Segoufin: *Tree languages defined in first-order logic with one quantifier alternation*

Gehrke, Grigorieff, Pin: *Duality and equational theory of regular languages*

Public-key Cryptography/ Authentication

Chairs: Vladimir Kolesnikov/Bartosz Przydatek

Prabhakaran, Rosulek: *Homomorphic Encryption with CCA Security*

Gilbert, Robshaw, Seurin: *How to Encrypt with the LPN Problem*

Ding, Yang, Cheng, Chen, Dubois: *Could SFLASH be repaired?*

Kolesnikov, Rackoff: *Password Mistyping in Two-Factor-Authenticated Key Exchange*

Jarecki, Liu: *Affiliation-Hiding Envelope and Authentication Schemes*

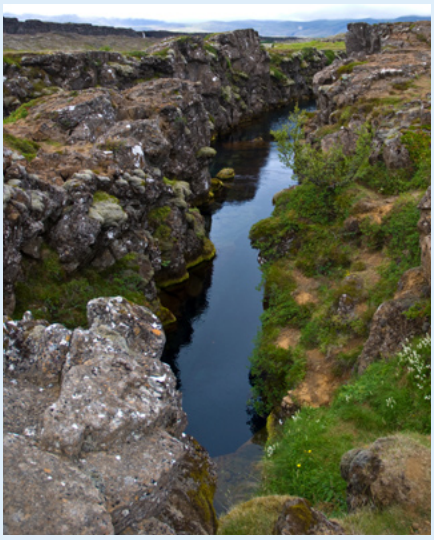
Track C concludes at 13:00

12:30 – 14:00 — *Lunch*

14:00 – 19:30

Excursion: Golden Circle afternoon tour

Early afternoon departure from Reykjavik. Our first stop will be at *Thingvellir National Park*. A UNESCO World Heritage site, Thingvellir National Park is of immense historic and symbolic importance to Icelanders. It was long the site of the original *Althing*, or national parliament of the settlers, and the setting for many of the most important events in the history of the island. Established in 930, the Althing was an assembly of free men that gathered at Thingvellir for two weeks each summer to settle disputes, set laws and arrange marriages. Thingvellir is also renowned for its geological significance. The area is located on the Mid-Atlantic ridge, where the continents of Europe and America drift apart, causing earthquakes and volcanic activity. Standing in the *Almannagjá* fissure, the visitor is literally situated between the continental plates. Thingvellir is also known for its exquisite beauty. The birch-covered lava fields and the clear blue waters of Lake Thingvallavatn produce a harmonious, almost serene landscape.



At Thingvellir. Photo by Tom Quine

From Thingvellir via Lyngdalsheidi plateau and Laugarvatn school village to *Gullfoss* waterfall, the Geysir hot springs area and Thingvellir National Park. Gullfoss, or the "Golden Waterfall" as the name implies, is located on the Hvitá river. The falls cascade 32m down in two stages. Often, colorful rainbows created by the sun on the spraying water can be enjoyed. The beauty of this waterfall can hardly be expressed fully in words. From Gullfoss to the geothermal field in Haukadalur is a natural wonder of hot springs and boiling mud pools. The "*Great Geyser*" even gave its name to this spectacular phenomenon. Today, the Geysir itself seldomly erupts, but nearby *Strokkur* sends up a column of water and steam up to 30 meters high every few minutes to the delight of onlookers.

Strokkur. Photo by Chris

On our way to Reykjavik we will make a short stop at *Kerid*, a lake-filled extinct volcanic crater. From there via Hveragerdi greenhouse village back to Reykjavik

All rooms are at Reykjavik University's main building at **Ofanleiti 2, 103 Reykjavik**
Further information and corrections on conference webpage: **http://www.ru.is/icalp08/**
Conference chairs: (+354) 845 6003 (Luca), (+354) 846 7919 (Anna), (+354) 825 6384 (Magnús)

Rooms 131 a & b
Room 231 a
Room 101
Room 201

ICALP 2008 Programme

Thursday, July 10th

	Track A *Algorithms, Automata, Complexity and Games* *(a)*	*(b)*	Track B *Logic, Semantics, and Theory of Programming*	Track C *Security and Cryptography Foundations*
09:00 – 10:00	**Invited talk: Peter Winkler, Dartmouth, USA** ***Optimality and Greed in Dynamic Allocation*** Chair: Leslie Ann Goldberg			
10:00 – 10:30	*Coffee break*			
10:30 – 12:30	**Graph algorithms** Chair: David Peleg Dragan, Fomin, Golovach: *Spanners in sparse graphs* Baswana, Gaur, Sen, Upadhyay: *Distance oracles for unweighted graphs: breaking the quadratic barrier with constant additive error* Roditty, Shapira: *All-Pairs Shortest Paths with a Sublinear Additive Error* Tedder, Corneil, Habib, Paul: *Simple Linear-Time Modular Decomposition Via Recursive Factorizing Permutations*	**Computational complexity** Chair: Josep Diaz Bulatov: *The Complexity of the Counting Constraint Satisfaction Problem* Krokhin, Marx: *On the hardness of losing weight* Lee, Mittal: *Product theorems via semidefinite programming* Ben-Sasson, Harsha, Lachish, Matsliah: *Sound 3-query PCPPs are Long*	**Nonstandard models of computation** Chair: Prakash Panangaden Yokoyama, Axelsen, Gluck: *Reversible Flowchart Languages and the Structured Reversible Program Theorem* Katsumata: *Attribute Grammars and Categorical Semantics* Martin: *A domain theoretic model of qubit channels* Coecke, Duncan: *Interacting Quantum Observables*	
12:30 – 14:00	*Lunch*			
14:00 – 16:00	**Games and automata** Chair: Paul Spirakis Esparza, Gawlitza, Kiefer, Seidl: *Approximative Methods for Monotone Systems of min-max-Polynomial Equations* Etessami, Wojtczak, Yannakakis: *Recursive Stochastic Games with Positive Rewards* Kähler, Wilke: *Complementation, Disambiguation, and Determinization of Büchi Automata Unified* Greco, Scarcello: *Tree Projections: Hypergraph Games and Minimality*	**Group testing, streaming, and quantum** Chair: Leslie Ann Goldberg Rothschild, Porat: *Explicit Non-Adaptive Combinatorial Group Testing Schemes* Guha, McGregor: *Tight Lower Bounds for Multi-Pass Stream Computation via Pass Elimination* Regev, Schiff: *Impossibility of a Quantum Speed-up with a Faulty Oracle* Hallgren, Harrow: *Superpolynomial speedups based on almost any quantum circuit*	**Reasoning about computation** Chair: Dale Miller Kesner: *Perpetuality for full and safe composition (in a constructive setting)* Lebresne: *A System F with call-by-name exceptions* Simmons, Pfenning: *Linear Logical Algorithms* Birkedal, Reus, Schwinghammer, Yang: *A Simple Model of Separation Logic for Higher-order Store*	
16:00 – 16:30	*Coffee break*			
16:30 – 18:00	***Award Ceremony*** EATCS Award 2008 The EATCS Award is awarded in recognition of a distinguished career in theoretical computer science. The recipient of the 2008 EATCS Award is *Leslie G. Valiant* (Harvard, USA). *Laudatio delivered by David Peleg.* Gödel Prize 2008 The 2008 Gödel Prize for outstanding journal articles in the area of theoretical computer science, co-sponsored by EATCS and ACM SIGACT, will be awarded. The winner of the 2008 Gödel Prize is the paper *Smoothed analysis of algorithms: Why the simplex algorithm usually takes polynomial time* by *Daniel A. Spielman and Shang-Hua Teng*. *Laudatio delivered by Volker Diekert.*			
20:00 – 23:00	***Conference Banquet*** Dinner at Perlan			

All rooms are at Reykjavik University's main building at **Ofanleiti 2, 103 Reykjavik**
Further information and corrections on conference webpage: **http://www.ru.is/icalp08/**
Conference chairs: (+354) 845 6003 (Luca), (+354) 846 7919 (Anna), (+354) 825 6384 (Magnús)

Rooms 131 a & b
Room 231 a
Room 101
Room 201

ICALP 2008 Programme

Friday, July 11th

	Track A *Algorithms, Automata, Complexity and Games* *(a)*	*(b)*	Track B *Logic, Semantics, and Theory of Programming*	Track C *Security and Cryptography Foundations*
09:00 – 10:00	**Invited talk: Javier Esparza, Technische Universität München, Germany** ***Newtonian Program Analysis*** Chair: Igor Walukiewicz			
10:00 – 10:30	*Coffee break*			
10:30 – 12:30	**Algorithmic game theory** Chair: Kousha Etessami Fanelli, Flammini, Moscardelli: *The Speed of Convergence in Congestion Games under Best-Response Dynamics* Briest: *Uniform Budgets and the Envy-Free Pricing Problem* Schapira, Christodoulou, Kovacs: *Bayesian Combinatorial Auctions* Gamzu, Azar: *Truthful Unification Framework for Packing Integer Programs with Choices* *Track A (a) concludes at 12:30*	**Quantum** Chair: Peter Bro Miltersen Kempe, Regev, Unger, de Wolf: *Upper Bounds on the Noise Threshold for Fault-tolerant Quantum Computing* Mhalla, Perdrix: *Finding Optimal Flows Efficiently* Childs, Lee: *Optimal quantum adversary lower bounds for ordered search* Eldar, Regev: *Quantum SAT for a qutrit-cinquit pair is QMA_1-complete* *Track A (b) concludes at 12:30*	**Verification** Chair: Luca Aceto Greimel, Bloem, Jobstmann, Vardi: *Open Implication* Schewe: *ATL* Satisfiability is 2EXPTIME-Complete* Servais, Raskin: *Visibly Pushdown Transducers* Colcombet, Loeding: *The non-deterministic Mostowski hierarchy and distance-parity automata* Axelsson, Heljanko, Lange: *Analyzing Context-Free Grammars Using an Incremental SAT Solver* *Track B concludes at 13:00*	
12:30 – 14:00	*Lunch*			

All rooms are at Reykjavik University's main building at **Ofanleiti 2, 103 Reykjavik**
Further information and corrections on conference webpage: **http://www.ru.is/icalp08/**
Conference chairs: (+354) 845 6003 (Luca), (+354) 846 7919 (Anna), (+354) 825 6384 (Magnús)

Rooms 131 a & b
Room 231 a
Room 101
Room 201