

# *Proceedings*

---

## **Twenty-Third Annual IEEE Symposium on Logic in Computer Science**

*24–27 June 2008  
Pittsburgh, Pennsylvania*

**Sponsored by**  
IEEE Computer Society  
Technical Committee on Mathematical Foundations of Computing

**In cooperation with**  
Association for Symbolic Logic  
European Association for Theoretical Computer Science



Los Alamitos, California  
Washington • Tokyo



# Table of Contents

## LICS 2008

<b>Foreword</b> .....	<b>x</b>
<b>Committees</b> .....	<b>xi</b>
<b>Reviewers</b> .....	<b>xiii</b>

---

### Session 1 (Joint CSF/LICS)

#### Invited Talk

Cryptographically-Sound Protocol-Model Abstractions .....	3
<i>Christoph Sprenger and David Basin (Speaker)</i>	
On the Expressiveness and Complexity of Randomization in Finite State Monitors .....	18
<i>Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanthan</i>	
An Authorization Logic with Explicit Time .....	
<i>Henry DeYoung, Deepak Garg and Frank Pfenning (CSF)</i>	

### Session 2 (Joint CSF/LICS)

DKAL: Distributed-Knowledge Authorization Language .....	
<i>Yuri Gurevich and Itay Neeman (CSF)</i>	
Access-Control Policies via Belnap Logic: Effective and Efficient Composition and Analysis .....	
<i>Glenn Bruns and Michael Huth (CSF)</i>	
Evidence-Based Audit .....	
<i>Jeffrey Vaughan, Limin Jia, Karl Mazurak and Steve Zdancewic (CSF)</i>	

### Session 3: Logical Frameworks

Combining Generic Judgments with Recursive Definitions .....	33
<i>Andrew Gacek, Dale Miller, and Gopalan Nadathur</i>	
Mechanizing the Metatheory of LF .....	45
<i>Christian Urban, James Cheney, and Stefan Berghofer</i>	
Second-Order and Dependently-Sorted Abstract Syntax .....	57
<i>Marcelo Fiore</i>	
Structural Logical Relations .....	69
<i>Carsten Schürmann and Jeffrey Sarnat</i>	

## Session 4: Lambda Calculus

Types for Hereditary Permutators .....	83
<i>Makoto Tatsuta</i>	
Context Matching for Compressed Terms .....	93
<i>Adrià Gascón, Guillem Godoy, and Manfred Schmidt-Schauss</i>	

## Session 5: Short Talks (Joint CSF/LICS)

Reducing Protocol Analysis with XOR to the XOR-free Case in the Horn Theory Based Approach	
<i>Ralf Küsters and Tomasz Truderung</i>	
A Proof Theoretic Analysis of Intruder Theories	
<i>Alwen Tiu and Rajeev Goré</i>	
Celf – A Logical Framework for Deductive and Concurrent Systems	
<i>Anders Schack-Nielsen and Carsten Schürmann</i>	
Improving Security Despite Compromise with Zero-Knowledge	
<i>Michael Backes, Catalin Hritcu, Matteo Maffei, and Dominique Unruh</i>	
A Formal Language for Cryptographic Pseudocode	
<i>Michael Backes, Matthias Berg, and Dominique Unruh</i>	
Testing Decision Procedures for Security-by-Contract	
<i>Nataliia Bielova, Fabio Massacci, and Ida Sri Rejeki Siahaan</i>	
The Maude-NRL Protocol Analyzer	
<i>Santiago Escobar, Catherine Meadows, and Jose Meseguer</i>	
Towards End-to-End Security Analysis of Networked Systems	
<i>Deepak Garg, Jason Franklin, Dilsun Kaynar, and Anupam Datta</i>	

## Session 6: Algebraic Reasoning

### Invited Talk

Nonlocal Flow of Control and Kleene Algebra with Tests .....	105
<i>Dexter Kozen</i>	
A Logic for Algebraic Effects .....	118
<i>Gordon Plotkin and Matija Pretnar</i>	
An Algebraic Process Calculus .....	130
<i>Emmanuel Beffara</i>	

## Session 7: Process Calculi

On the Expressiveness and Decidability of Higher-Order Process Calculi .....	145
<i>Ivan Lanese, Jorge A. Pérez, Davide Sangiorgi, and Alan Schmitt</i>	
On the Axiomatizability of Impossible Futures: Preorder versus Equivalence .....	156
<i>Taolue Chen and Wan Fokkink</i>	
General Structural Operational Semantics through Categorical Logic .....	166
<i>Sam Staton</i>	

## Session 8: Model Checking

Parameterization as Abstraction: A Tractable Approach to the Dataflow Analysis of Concurrent Programs.....	181
<i>Vineet Kahlon</i>	
Winning Regions of Higher-Order Pushdown Games.....	193
<i>A. Carayol, M. Hague, A. Meyer, C.-H. L. Ong, and O. Serre</i>	
The Ordinal Recursive Complexity of Lossy Channel Systems.....	205
<i>P. Chambart and P. Schnoebelen</i>	
Almost-Sure Model Checking of Infinite Paths in One-Clock Timed Automata.....	217
<i>Christel Baier, Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Marcus Größer</i>	

## Session 9: Proof Theory

From Axioms to Analytic Rules in Nonclassical Logics.....	229
<i>Agata Ciabattoni, Nikolaos Galatos, and Kazushige Terui</i>	
Focusing on Binding and Computation.....	241
<i>Daniel R. Licata, Noam Zeilberger, and Robert Harper</i>	
A First-Order Representation of Pure Type Systems Using Superdeduction.....	253
<i>Guillaume Burel</i>	

## Session 10: Computational Complexity

### Invited Talk

The Quest for a Logic Capturing PTIME.....	267
<i>Martin Grohe</i>	
On the Asymptotic Nullstellensatz and Polynomial Calculus Proof Complexity.....	272
<i>Søren Riis</i>	
On the Computational Complexity of Cut-Reduction.....	284
<i>Klaus Aehlig and Arnold Beckmann</i>	

## Session 11: Constraints

Maltsev + Datalog $\rightarrow$ Symmetric Datalog.....	297
<i>Victor Dalmau and Benoit Larose</i>	
Caterpillar Duality for Constraint Satisfaction Problems.....	307
<i>Catarina Carvalho, Victor Dalmau, and Andrei Krokhin</i>	
Quantified Constraints and Containment Problems.....	317
<i>Hubie Chen, Florent Madelaine, and Barnaby Martin</i>	

## Session 12: Reasoning About Programs

Hiding Local State in Direct Style: A Higher-Order Anti-Frame Rule .....	331
<i>François Pottier</i>	
Typed Normal Form Bisimulation for Parametric Polymorphism .....	341
<i>Soren B. Lassen and Paul Blain Levy</i>	
Reachability Games and Game Semantics: Comparing Nondeterministic Programs.....	353
<i>Andrzej S. Murawski</i>	
Weak Topology and a Differentiable Operator for Lipschitz Maps .....	364
<i>Abbas Edalat</i>	

## Session 13: Probabilistic Systems

A Logical Characterization of Individual-Based Models .....	379
<i>James F. Lynch</i>	
The Satisfiability Problem for Probabilistic CTL.....	391
<i>Tomáš Brázdil, Vojtěch Forejt, Jan Křetínský, and Antonín Kučera</i>	

## Session 14: Finite Model Theory

### Invited Talk

The Axiomatic Derivation of Absolute Lower Bounds .....	405
<i>Yiannis N. Moschovakis</i>	
Definable Tree Decompositions .....	406
<i>Martin Grohe</i>	
Hypergraph Acyclicity and Extension Preservation Theorems .....	418
<i>David Duris</i>	

## Session 15: Automata Theory

From Automatic Structures to Borel Structures.....	431
<i>Greg Hjorth, Bakh Khoussainov, Antonio Montalbán, and André Nies</i>	
Piecewise Testable Tree Languages .....	442
<i>Mikołaj Bojańczyk, Luc Segoufin, and Howard Straubing</i>	
Collapsible Pushdown Automata and Recursion Schemes.....	452
<i>M. Hague, A.S. Murawski, C.-H.L. Ong, and O. Serre</i>	

## **Session 16: Linear Logic**

The Geometry of Interaction of Differential Interaction Nets .....	465
<i>Marc de Falco</i>	
Correctness of Multiplicative Additive Proof Structures is <i>NL</i> -Complete .....	476
<i>Paulin Jacobé de Naurois and Virgile Mogbil</i>	
Cut Elimination for Monomial MALL Proof Nets .....	486
<i>Olivier Laurent and Roberto Maieli</i>	
A Neutral Approach to Proof and Refutation in MALL .....	498
<i>Olivier Delandé and Dale Miller</i>	
<b>Author Index</b> .....	509