

2016 Formal Methods in Computer-Aided Design (FMCAD 2016)

**Mountain View, California, USA
3-6 October 2016**



**IEEE Catalog Number: CFP16FMC-POD
ISBN: 978-1-5386-2692-4**

**Copyright © 2016, FMCAD Inc.
All Rights Reserved**

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP16FMC-POD
ISBN (Print-On-Demand):	978-1-5386-2692-4
ISBN (Online):	978-0-9835678-6-8

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

Table of Contents

Formal Verification for Computer Security: Lessons Learned and Future Directions.....	1
<i>Dawn Song</i>	
Understanding Evolution through Algorithms	2
<i>Christos Papadimitriou</i>	
Network Verification - When Clarke Meets Cerf	3
<i>George Varghese</i>	
Machine Learning and Systems for the Next Frontier in Formal Verification	4
<i>Manish Pandey</i>	
Verifying Hyperproperties of Hardware Systems	5
<i>Bernd Finkbeiner and Markus Rabe</i>	
A Paradigm Shift in Verification Methodology	6
<i>Pranav Ashar</i>	
Program Synthesis for Networks	7
<i>Pavol Černý</i>	
The FMCAD 2016 Graduate Student Forum	8
<i>Hossein Hojjat</i>	
Soundness of the Quasi-Synchronous Abstraction	9
<i>Guillaume Baudart, Timothy Bourke and Marc Pouzet</i>	
Synthesizing Adaptive Test Strategies from Temporal Logic Specifications	17
<i>Roderick Bloem, Robert Koenighofer, Ingo Pill and Franz Roeck</i>	
Reducing Interpolant Circuit Size by Ad Hoc Logic Synthesis and SAT-Based Weakening	25
<i>Gianpiero Cabodi, Paolo E. Camurati, Marco Palena, Paolo Pasini and Danilo Vendramineto</i>	
Extracting Behaviour from an Executable Instruction Set Model	33
<i>Brian Campbell and Ian Stark</i>	
Categorical Semantics of Digital Circuits	41
<i>Dan Ghica and Achim Jung</i>	
Equivalence Checking By Logic Relaxation	49
<i>Eugene Goldberg</i>	
Minimal unsatisfiable core extraction for SMT	57
<i>Ofer Guthmann, Ofer Strichman and Anna Trostanetski</i>	
Efficient Uninterpreted Function Abstraction and Refinement for Word-level Model Checking	65
<i>Yen-Sheng Ho, Pankaj Chauhan, Pritam Roy, Alan Mishchenko and Robert Brayton</i>	
Optimizing Horn Solvers for Network Repair	73
<i>Hossein Hojjat, Philipp Ruemmer, Jedidiah McClurg, Pavol Černý and Nate Foster</i>	
On $\exists\forall\exists!$ Solving: A Case Study on Automated Synthesis of Magic Card Tricks	81
<i>Susmit Jha, Vasumathi Raman and Sanjit A. Seshia</i>	
Property-Directed k-Induction	85
<i>Dejan Jovanović and Bruno Dutertre</i>	
Lazy Proofs for DPLL(T)-Based SMT Solvers	93
<i>Guy Katz, Clark Barrett, Cesare Tinelli, Andrew Reynolds and Liana Hadarean</i>	
Verifiable Hierarchical Protocols with Network Invariants on Parametric Systems	101
<i>Opeoluwa Matthews, Jesse Bingham and Daniel Sorin</i>	

Modular Specification and Verification of a Cache-Coherent Interface	109
<i>Kenneth McMillan</i>	
Proof Certificates for SMT-based Model Checkers for Infinite-state Systems	117
<i>Alain Mebsout and Cesare Tinelli</i>	
Routing under Constraints	125
<i>Alexander Nadel</i>	
A Consistency Checker for Memory Subsystem Traces	133
<i>Matthew Naylor, Simon Moore and Alan Mujumdar</i>	
Hybrid Partial Order Reduction with Under-Approximate Dynamic Points-To and Determinacy Information	141
<i>Pavel Parizek</i>	
Formal Verification of Division and Square Root Implementations, an Oracle Report	149
<i>David Rager, Jo Ebergen, Dmitry Nadezhin, Austin Lee, Cuong Chau and Ben Selfridge</i>	
Integrating Proxy Theories and Numeric Model Lifting for Floating-Point Arithmetic	153
<i>Jaideep Ramachandran and Thomas Wahl</i>	
Trustworthy Specifications of ARM v8-A and v8-M System Level Architecture	161
<i>Alastair Reid</i>	
Equivalence Checking Using Gröbner Bases	169
<i>Amr Sayed-Ahmed, Daniel Grosse, Mathias Soeken and Rolf Drechsler</i>	
Accurate ICP-based Floating-Point Reasoning	177
<i>Karsten Scheibler, Felix Neubauer, Ahmed Mahdi, Martin Fränzle, Tino Teige, Tom Bienmüller, Detlef Fehrer and Bernd Becker</i>	
SWAPPER: A Framework for Automatic Generation of Formula Simplifiers based on Conditional Rewrite Rules	185
<i>Rohit Singh and Armando Solar-Lezama</i>	
Lazy Sequentialization for TSO and PSO via Shared Memory Abstractions	193
<i>Ermenegildo Tomasco, Truc Nguyen Lam, Omar Inverso, Bernd Fischer, Salvatore La Torre and Gennaro Parlato</i>	
Combining Requirement Mining, Software Model Checking, and Simulation-Based Verification for Industrial Automotive Systems	201
<i>Tomoya Yamaguchi, Tomoyuuki Kaga, Alexandre Donzé and Sanjit A Seshia</i>	