

2017 Formal Methods in Computer Aided Design (FMCAD 2017)

**Vienna, Austria
2-6 October 2017**



**IEEE Catalog Number: CFP17FMC-POD
ISBN: 978-1-5386-1012-1**

**Copyright © 2017, 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:	CFP17FMC-POD
ISBN (Print-On-Demand):	978-1-5386-1012-1
ISBN (Online):	978-0-9835678-7-5

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

Invited Papers

How formal analysis and verification add security to blockchain-based systems	1
<i>Shin'Ichiro Matsuo</i>	
Symbolic Security Analysis using the Tamarin Prover	5
<i>Cas Cremers</i>	
Coalition, intrigue, ambush, destruction and pride: herding cats can be challenging	6
<i>Jade Alglave</i>	
Automated Formal Reasoning About AWS Systems	7
<i>Byron Cook</i>	
Formal Methods in Industrial Dependable Systems Design - The TTTech Example	8
<i>Wilfried Steiner</i>	
Hardware Model Checking Competition 2017	9
<i>Armin Biere, Tom van Dijk and Keijo Heljanko</i>	
The FMCAD 2017 Graduate Student Forum	10
<i>Keijo Heljanko</i>	

Arithmetic

goSAT: Floating-point Satisfiability as Global Optimization	11
<i>M. Ammar Ben Khadra, Dominik Stoffel and Wolfgang Kunz</i>	
On Sound Relative Error Bounds for Floating-Point Arithmetic	15
<i>Anastasiia Izycheva and Eva Darulova</i>	
Column-Wise Verification of Multipliers Using Computer Algebra	23
<i>Daniela Ritirc, Armin Biere and Manuel Kauers</i>	

Solving

Efficient Generation of All Minimal Inductive Validity Cores	31
<i>Elaheh Ghassabani, Michael Whalen and Andrew Gacek</i>	
Duality-Based Interpolation for Quantifier-Free Equalities and Uninterpreted Functions	39
<i>Leonardo Alt, Antti Hyvärinen, Sepideh Asadi and Natasha Sharygina</i>	
Solving Linear Arithmetic with SAT-based Model Checking	47
<i>Yakir Vizel, Alexander Nadel and Sharad Malik</i>	
Z3str3: A String Solver with Theory-aware Heuristics	55
<i>Murphy Berzish, Vijay Ganesh and Yunhui Zheng</i>	

Concurrency and Distributed Systems

Verification of a lazy cache coherence protocol against a weak memory model	60
<i>Christopher Banks, Marco Elver, Ruth Hoffmann, Susmit Sarkar, Paul Jackson and Vijay Nagarajan</i>	
Safety Verification of Phaser Programs	68
<i>Zeinab Ganjei, Ahmed Rezine, Petru Eles and Zebo Peng</i>	
Learning to prove safety over parameterised concurrent systems	76
<i>Yu-Fang Chen, Chih-Duo Hong, Anthony Widjaja Lin and Philipp Ruemmer</i>	
Lasso detection using Partial State Caching	84
<i>Rashmi Mudduluru, Pantazis Deligiannis, Ankush Desai, Akash Lal and Shaz Qadeer</i>	

Probabilistic Systems

Exact Quantitative Probabilistic Model Checking Using Rational Search	92
<i>Matthew S. Bauer, Umang Mathur, Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan</i>	

Sampling Invariants from Frequency Distributions	100
<i>Grigory Fedyukovich, Samuel Kaufman and Rastislav Bodik</i>	
BDDs	
Tagged BDDs: Combining reduction rules from different decision diagram types	108
<i>Tom van Dijk, Robert Wille and Robert Meolic</i>	
First-order Temporal Logic Monitoring with BDDs	116
<i>Klaus Havelund, Doron Peled and Dogan Ulus</i>	
Factored Boolean Functional Synthesis	124
<i>Lucas Martinelli Tabajara and Moshe Y. Vardi</i>	
IC3	
Property Directed Reachability with Word-Level Abstraction	132
<i>Yen-Sheng Ho, Alan Mishchenko and Robert Brayton</i>	
Learning Support Sets in IC3 and Quip: the Good, the Bad, and the Ugly	140
<i>Ryan Berryhill, Alexander Ivrii, Neil Veira and Andreas Veneris</i>	
K-Induction without Unrolling	148
<i>Arie Gurfinkel and Alexander Ivrii</i>	
Designing Parallel PDR	156
<i>Matteo Marescotti, Arie Gurfinkel, Antti Hyvärinen and Natasha Sharygina</i>	
FuseIC3: An Algorithm for Checking Large Design Spaces	164
<i>Rohit Dureja and Kristin Yvonne Rozier</i>	
FAR-Cubicle - A new reachability algorithm for Cubicle	172
<i>Sylvain Conchon, Amit Goel, Sava Krstic, Rupak Majumdar and Mattias Roux</i>	
Theta: a Framework for Abstraction Refinement-Based Model Checking	176
<i>Tamás Tóth, Ákos Hajdu, András Vörös, Zoltán Micskei and István Majzik</i>	
Hybrid Systems	
Modular SMT-Based Analysis of Nonlinear Hybrid Systems	180
<i>Kyungmin Bae and Sicun Gao</i>	
SMT-based Analysis of Switching Multi-Domain Linear Kirchhoff Networks	188
<i>Alessandro Cimatti, Sergio Mover and Mirko Sessa</i>	
Applications	
Automatic Verification of Application-Tailored OSEK Kernels	196
<i>Hans-Peter Deifel, Christian Dietrich, Merlin Göttlinger, Daniel Lohmann, Stefan Milius and Lutz Schröder</i>	
Estimating Worst-case Latency of on-chip Interconnects with Formal Simulation	204
<i>Freek Verbeek and Nike van Vugt-Hage</i>	
Parameterized Verification of Algorithms for Oblivious Robots on a Ring	212
<i>Arnaud Sangnier, Nathalie Sznajder, Maria Potop-Butucaru and Sebastien Tixeuil</i>	
Automated Repair By Example for Firewalls	220
<i>William Hallahan, Ennan Zhai and Ruzica Piskac</i>	