2021 Formal Methods in Computer Aided Design (FMCAD 2021)

Virtual Conference
19 – 22 October 2021

IEEE

IEEE Catalog Number: CFP21FMC-POD
ISBN: 978-1-6654-0294-1

****** 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:	CFP21FMC-POD
ISBN (Print-On-Demand):	978-1-6654-0294-1
ISBN (Online):	978-3-85448-046-4
ISSN:	2641-8177

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

Table of Contents

Tutorials

Reactive Synthesis Beyond Realizability 1
Rayna Dimitrova

Stainless Verification System Tutorial 2
Viktor Kuncak and Jad Hamza

Formal Methods for the Security Analysis of Smart Contracts 8
Matteo Maffei

Active Automata Learning: from L* to L# 9
Frits Vaandrager

Invited Talks

From Viewstamped Replication to Blockchains 10
Barbara Liskov

Algorithms for the People 11
Seny Kamara

Engineering with Full-scale Formal Architecture: Morello, CHERI, Armv8-A, and RISC-V 12
Peter Sewell

Student Forum

The FMCAD 2021 Student Forum 13
Mark Santolucito

Hardware

CocoAlma: A Versatile Masking Verifier 14
Vedad Hadžić and Roderick Bloem

End-to-End Formal Verification of a RISC-V Processor Extended with Capability Pointers 24
Dapeng Gao and Tom Melham

Hardware Security Leak Detection by Symbolic Simulation 34
Neta Bar Kama and Roope Kaivola

Scaling Up Hardware Accelerator Verification using A-QED with Functional Decomposition 42
Saranyu Chattopadhyay, Florian Lonsing, Luca Piccolboni, Deepraj Soni, Peng Wei, Xiaofan Zhang, Yuan Zhou, Luca Carloni, Deming Chen, Jason Cong, Ramesh Karri, Zhiru Zhang, Caroline Trippel, Clark Barrett and Subhasish Mitra

Sound and Automated Verification of Real-World RTL Multipliers 53
Mertcan Temel and Warren Hunt

Model Checking and IC3

IC3 with Internal Signals 63
Rohit Dureja, Arie Gurfinkel, Alexander Ivrii and Yakir Vizel

Single Clause Assumption without Activation Literals to Speed-up IC3 72
Nils Froleyks and Armin Biere

Logical Characterization of Coherent Uninterpreted Programs 77
Hari Govind Vediramana Krishnan, Sharon Shoham and Arie Gurfinkel

Data-driven Optimization of Inductive Generalization 86
Nham Le, Xujie Si and Arie Gurfinkel

Model Checking AUTOSAR Components with CBMC 96
Timothee Durand, Katalin Fazekas, Georg Weissenbacher and Jakob Zwirchmayr

Concurrency and Distributed Systems

Automating System Configuration 102
Nestan Tsiskaridze, Maxwell Strange, Makai Mann, Kavya Sreedhar, Qiaoyi Liu, Mark Horowitz and Clark Barrett

Towards an Automatic Proof of Lamport's Paxos 112
Aman Goel and Karem A. Sakallah

Refinement-Based Verification of Device-to-Device Information Flow 123
Ning Dong, Roberto Guanciale and Mads Dam

Celestial: A Smart Contracts Verification Framework 133
Samvid Dharanikota, Suvam Mukherjee, Chandrika Bhardwaj, Aseem Rastogi and Akash Lal

The Civl Verifier 143
Bernhard Kragl and Shaz Qadeer

Applied Verification and Synthesis

Synthesizing Pareto-Optimal Interpretations for Black-Box Models 153
Hazem Torfah, Shetal Shah, Supratik Chakraborty, S. Akshay and Sanjit A. Seshia

Dynamic Partial Order Reduction for Spinloops 163
Michalis Kokologiannakis, Xiaowei Ren and Viktor Vafeiadis

Robustness between Weak Memory Models 173
Soham Chakraborty

Pruning and Slicing Neural Networks using Formal Verification 183
Ori Lahav and Guy Katz

Towards Scalable Verification of Deep Reinforcement Learning 193
Guy Amir, Michael Schapira and Guy Katz

SAT Solving

Exploiting Isomorphic Subgraphs in SAT 204
Alexander Ivrii and Ofer Strichman

On Decomposition of Maximal Satisfiable Subsets 212
Jaroslav Bendík

Designing Samplers is Easy: The Boon of Testers 222
Priyanka Golia, Mate Soos, Sourav Chakraborty and Kuldeep S. Meel

SAT-Inspired Eliminations for Superposition 231
Petar Vukmirović, Jasmin Blanchette and Marijn Heule

SAT Solving in the Serverless Cloud 241
Alex Ozdemir, Haoze Wu and Clark Barrett

SMT and First-Order Logic

Induction with Recursive Definitions in Superposition 246
Marton Hajdu, Petra Hozzová, Laura Kovacs and Andrei Voronkov

Fair and Adventurous Enumeration of Quantifier Instantiations 256
Mikolas Janota, Haniel Barbosa, Pascal Fontaine and Andrew Reynolds

Mathematical Programming Modulo Strings 261
Ankit Kumar and Panagiotis Manolios

Lookahead in Partitioning SMT 271
Antti Hyvärinen, Matteo Marescotti and Natasha Sharygina

A Multithreaded Vampire with Shared Persistent Grounding 280
Michael Rawson and Giles Reger