Ruzica Piskac / Michael W. Whalen (Eds.)
PROCEEDINGS OF THE 21ST CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2021

Conference Series: Formal Methods in Computer-Aided Design
Volume 2

Conference Series: Formal Methods in Computer-Aided Design

Series edited by:
Warren A. Hunt, Jr., The University of Texas at Austin
Austin, TX 78705 | hunt@cs.utexas.edu
Georg Weissenbacher, TU Wien
Karlsplatz 13, 1040 Wien, Austria | georg.weissenbacher@tuwien.ac.at

The Conference on Formal Methods in Computer-Aided Design (FMCAD) is an annual conference on the theory and applications of formal methods in hardware and system verification. FMCAD provides a leading forum to researchers in academia and industry for presenting and discussing groundbreaking methods, technologies, theoretical results, and tools for reasoning formally about computing systems. FMCAD covers formal aspects of computer-aided system design including verification, specification, synthesis, and testing.

Information on this publication series and the volumes published therein is available at www.tuwien.ac.at/academicpress.

Volume 2 edited by:
Ruzica Piskac, Yale University
51 Prospect Street, New Haven, CT 06511, USA | ruzica.piskac@yale.edu
Michael W. Whalen, Amazon Web Services, Inc.
323 N Washington Ave, Minneapolis, MN 55401, USA | mww@amazon.com

Ruzica Piskac / Michael W. Whalen (Eds.)

PROCEEDINGS OF THE 21ST CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2021

TU WIEN Academic Press

Cite as:
Piskac, R. & Whalen, M. W. (Eds.). (2021). *Proceedings of the 21st Conference on Formal Methods in Computer-Aided Design – FMCAD 2021*. TU Wien Academic Press. https://doi.org/10.34727/2021/isbn.978-3-85448-046-4

TU Wien Academic Press, 2021

c/o TU Wien Bibliothek
TU Wien
Resselgasse 4, 1040 Wien
academicpress@tuwien.ac.at
www.tuwien.at/academicpress

ISBN (online): 978-3-85448-046-4
ISSN (online): 2708-7824

Available online: https://doi.org/10.34727/2021/isbn.978-3-85448-046-4

Media proprietor: TU Wien, Karlsplatz 13, 1040 Wien
Publisher: TU Wien Academic Press
Publication series editor: Warren A. Hunt, Jr. and Georg Weissenbacher
Editors (responsible for the content): Ruzica Piskac and Michael W. Whalen

Preface

These are the proceedings of the twenty-first International Conference on Formal Methods in Computer-Aided Design (FMCAD), which was held online from October 18 – October 22, 2021 due to the coronavirus. FMCAD was constituted in 1996 as a conference covering formal aspects of specification, verification, synthesis, testing, and security, and as a leading forum for researchers and practitioners in academia and industry alike. 2021 marks the 25th anniversary of that original meeting, and so we wish to celebrate the vision of those original organizers!

The program of FMCAD 2021 is comprised of four tutorials, three invited talks, a student forum, an industry night, a panel session on "25 years of FMCAD", and the main program consisting of presentations of 30 accepted papers. The tutorial day featured four presentations:

- *Active Automata Learning: from L^* to $L^\#$* by Frits Vaandrager
- *Stainless Verification System Tutorial* by Viktor Kuncak
- *Reactive Synthesis Beyond Realizability* by Rayna Dimitrova
- *Formal Methods for the Security Analysis of Smart Contracts* by Matteo Maffei

and the main conference featured three invited talks:

- *From Viewstamped Replication to Blockchains* by Barbara Liskov
- *Algorithms for the People* by Seny Kamara
- *Engineering with Full-scale Formal Architecture: Morello, CHERI, Armv8-A, and RISC-V* by Peter Sewell

FMCAD'21 also hosted the ninth edition of the Student Forum, which has been held annually since 2013 and provides a platform for graduate students at any career stage to introduce their research to the FMCAD community. The FMCAD Student Forum 2021 was organized by Mark Santolucito and featured short presentations of 11 accepted contributions. A detailed description of the Student Forum, listing all accepted contributions, is provided in the conference proceedings. FMCAD 2021 received 72 submissions out of which the committee decided to accept 30 for publication. Each submission received at least three reviews. The topics of the accepted papers include hardware and software verification, SAT, SMT, learning, synthesis, Neural-Network verification, and more. Out of the accepted papers, 23 are classified as regular papers (20 long and 3 short) and 7 are classified as tool/case study papers (5 long and 2 short).

Organizing this event would not have been possible without the support of a large number of people and our sponsors. The program committee members and additional reviewers, listed on the following pages, did an excellent job providing detailed and insightful reviews, which helped the authors to improve their submissions and guided the selection of the papers accepted for publication. We thank each and everyone of them for dedicating their time and providing their expertise. We thank William Hallahan (Yale University) for being the web master, Daniel Schoepe for being the Sponsorship Chair, and Mark Santolucito for organizing this year's FMCAD Student Forum. We thank Georg Weissenbacher (TU Wien) both for his exceptional assistance in organizing the event, communicating to us the decisions of the steering committee, as well as being the publication chair. Holding a conference like FMCAD would not be feasible without the financial support of our sponsors. We would like to express our gratitude to our sponsors (in alphabetical order): Amazon Web Services, Amazon Prime Video, Cadence, Centaur Technology, Galois, Intel, Mentor Graphics, Novi, and Synopsys.

The conference proceedings are available as Open Access Proceedings published by TU Wien Academic Press, and through the IEEE Xplore Digital Library. Last but not least, we thank all authors who submitted their papers to FMCAD 2021 (accepted or not), and whose contributions and presentations form the core of the conference. We are grateful to everyone who presented their paper, gave a keynote or gave a tutorial. We thank all attendees of FMCAD for supporting the conference and making FMCAD a stimulating and enjoyable event.

October, 2021

Ruzica Piskac, Yale University
Michael W. Whalen, Amazon Inc. and the University of Minnesota

Organizing Committee

Program Co-Chairs

Ruzica Piskac	Yale University
Michael W. Whalen	Amazon Inc. and the University of Minnesota

Webmaster

William Hallahan	Yale University

Student Forum Chair

Mark Santolucito	Barnard College of Columbia University

Publication Chair

Georg Weissenbacher	TU Wien

Steering Committee

Clark Barrett	Stanford University
Armin Biere	Johannes Kepler University Linz
Anna Slobodova	Centaur Technology
Georg Weissenbacher	TU Wien

Program Committee

Erika Abraham	RWTH Aachen University
Jade Alglave	University College London
Pranav Ashar	Real Intent
Per Bjesse	Synopsys
Roderick Bloem	Graz University of Technology
Ivana Cerna	Masaryk University
Supratik Chakraborty	IIT Bombay
Sylvain Conchon	Université Paris-Sud
Leonardo de Moura	Microsoft
Rayna Dimitrova	CISPA Helmholtz Center for Information Security
Grigory Fedyukovich	Florida State University
Arie Gurfinkel	University of Waterloo
Liana Hadarean	Amazon Web Services
Ziyad Hanna	Cadence Design System
Fei He	Tsinghua University
Marijn Heule	Carnegie Mellon University
Warren A. Hunt, Jr.	The University of Texas at Austin
Alexander Ivrii	IBM
Dejan Jovanović	Amazon Web Services
Alan Jovic	University of Zagreb
Laura Kovacs	TU Wien
Ton Chanh Le	Stevens Institute of Technology
Rebekah Leslie-Hurd	Intel
Kuldeep S. Meel	National University of Singapore
Ruzica Piskac	Yale University
Elizabeth Polgreen	University of California, Berkeley
Andrew Reynolds	University of Iowa
Christoph Scholl	University of Freiburg
Natasha Sharygina	Università della Svizzera italiana (USI Lugano, Switzerland)
Anna Slobodova	Centaur Technology
Christoph Sticksel	The MathWorks
Murali Talupur	Amazon Web Services, Inc.
Jean-Baptiste Tristan	Boston College
Yakir Vizel	The Technion
Thomas Wahl	Northeastern University
Georg Weissenbacher	TU Wien
Michael Whalen	Amazon Inc. and the University of Minnesota
Thomas Wies	New York University
Valentin Wüstholz	ConsenSys
Lenore Zuck	University of Illinois in Chicago

Additional Reviewers

Asadi, Sepideh
Athanasiou, Konstantinos

Bansal, Suguman
Barnett, Lee
Bendík, Jaroslav
Blicha, Martin
Bustan, Doron

Cano, Filip
Chalupa, Marek
Cheang, Kevin
Chen, Hao
Chernigovskaia, Lidiia

Ebrahimi, Masoud

Fan, Hongyu
Fernandez, Matt
Fraer, Ranan

Georgiou, Pamina
Goel, Shilpi
Golia, Priyanka
Grundy, Jim

Hamza, Ameer
Hjort, Håkan
Hoereth, Stefan
Hozzová, Petra
Huang, Daniel
Hyvärinen, Antti

Jacoby, Reily
Jain, Himanshu
Jain, Mitesh
Jin, Hoon Sang
Jonas, Martin

Könighofer, Bettina
Kwan, Carl

Larrauri, Alberto
Le, Nham

Maderbacher, Benedikt
Majumdar, Rupak
Moosbrugger, Marcel
Mora, Federico

Nalbach, Jasper

Otoni, Rodrigo

Ramanathan, Vivek
Rane, Ashay
Reeves, Joseph
Rehak, Vojtech
Ročkai, Petr

Santolucito, Mark
Schoisswohl, Johannes
Seufert, Tobias
Shi, Yunong
Soos, Mate
Stankovic, Miroslav
Strejček, Jan
Strichman, Ofer
Sumners, Rob
Swords, Sol

Tassarotti, Joseph
Temel, Mertcan

Vediramana Krishnan, Hari Govind

Wolfovitz, Guy

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