

Formal Methods

LNCS 13274

Maurice H. ter Beek
Rosemary Monahan (Eds.)

Integrated Formal Methods

**17th International Conference, IFM 2022
Lugano, Switzerland, June 7–10, 2022
Proceedings**



Springer

Founding Editors

Gerhard Goos, Germany
Juris Hartmanis, USA

Editorial Board Members

Elisa Bertino, USA
Wen Gao, China

Bernhard Steffen , Germany
Moti Yung , USA

Formal Methods

Subline of Lectures Notes in Computer Science

Subline Series Editors

Ana Cavalcanti, *University of York, UK*
Marie-Claude Gaudel, *Université de Paris-Sud, France*

Subline Advisory Board

Manfred Broy, *TU Munich, Germany*
Annabelle McIver, *Macquarie University, Sydney, NSW, Australia*
Peter Müller, *ETH Zurich, Switzerland*
Erik de Vink, *Eindhoven University of Technology, The Netherlands*
Pamela Zave, *AT&T Laboratories Research, Bedminster, NJ, USA*


More information about this series at <https://link.springer.com/bookseries/558>


Maurice H. ter Beek · Rosemary Monahan (Eds.)

Integrated Formal Methods

17th International Conference, IFM 2022
Lugano, Switzerland, June 7–10, 2022
Proceedings

Editors

Maurice H. ter Beek 
ISTI-CNR
Pisa, Italy

Rosemary Monahan 
Maynooth University
Maynooth, Ireland

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-07726-5

ISBN 978-3-031-07727-2 (eBook)

<https://doi.org/10.1007/978-3-031-07727-2>

© Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers presented at the 17th International Conference on integrated Formal Methods (iFM 2022) held in beautiful Lugano, Switzerland, and hosted by the Software Institute of the Università della Svizzera italiana (USI). These proceedings also contain seven papers selected by the Program Committee of the PhD Symposium (PhD-iFM 2022) chaired by Marie Farrell and João F. Ferreira.

In recent years, we have witnessed a proliferation of approaches that integrate several modeling, verification, and simulation techniques, facilitating more versatile and efficient analysis of software-intensive systems. These approaches provide powerful support for the analysis of different functional and non-functional properties of the systems, and the complex interaction of components of different nature, as well as validation of diverse aspects of system behavior. The iFM conference series is a forum for discussing recent research advances in the development of integrated approaches to formal modeling and analysis. The conference series covers all aspects of the design of integrated techniques, including language design, verification and validation, automated tool support, and the use of such techniques in software engineering practice.

iFM 2022 solicited high-quality papers reporting research results and/or experience reports related to the overall theme of formal methods integration. The Program Committee (PC) originally received a total of 53 abstract submissions, which eventually resulted in 46 paper submissions from authors in 24 different countries spread over all six continents: 40 regular papers, five short papers, and one journal-first paper submission. Each submission went through a rigorous review process according to which all papers were reviewed by three PC members, with the help of many external reviewers, followed by a short yet intense discussion phase. The decision to accept or reject a paper was based not only on the review reports and scores but also, and in particular, on these in-depth discussions. In the end, the PC of iFM 2022 selected 16 papers for presentation during the conference and inclusion in these proceedings: 14 regular papers, one short paper, and one journal-first paper. This amounts to an overall acceptance rate of 34.8% (35% for regular papers and 20% for short papers). The PC of PhD-iFM 2022 received eight submissions and selected seven papers for presentation during the conference and inclusion in these proceedings.

To credit the effort of tool developers, this edition of iFM introduced for the first time EAPLS artifact badging. The Artifact Evaluation Committee, chaired by Alessio Ferrari and Marie-Christine Jakobs, received seven submissions and worked hard to run often complex tools and long experiments. All artifacts achieved the available and the functional badge, while two artifacts of particularly good quality were awarded the functional and reusable badge.

The conference featured keynotes by Yamine Aït Ameer (Toulouse INP and IRIT-CNRS, France), Roderick Bloem (Graz University of Technology, Austria), and—as a joint keynote speaker of iFM 2022 and PhD-iFM 2022—Louise Dennis (University of Manchester, UK). We hereby heartily thank these invited speakers.

We are grateful to all involved in iFM 2022. In particular, all PC members and external reviewers for their accurate and timely reviewing, all authors for their submissions, and all attendees for their participation. We also thank all chairs and committees (Journal First Track, Artifact Evaluation Committee, and PhD Symposium), itemized on the following pages, and the excellent local organization and finance and publicity teams chaired by Carlo A. Furia.

We are very grateful to the organizations which sponsored the conference: The Hasler Foundation, Springer, and the European Association for Programming Languages and Systems (EAPLS).

Finally, we thank Springer for publishing these proceedings in their FM subline, and for facilitating the EAPLS artifact badges on the papers, and we kindly acknowledge the support from EasyChair in assisting us in managing the complete process from submissions through these proceedings to the program.

We hope you enjoyed the conference!

April 2022

Maurice H. ter Beek
Rosemary Monahan

Anamaria Martins Moreira	Federal University of Rio de Janeiro, Brazil
Dominique Méry	Loria and University of Lorraine, France
Stephan Merz	Inria Nancy and Loria, France
Luigia Petre	Åbo Akademi University, Finland
André Platzer	Carnegie Mellon University, USA
Jaco van de Pol	Aarhus University, Denmark
Kostis Sagonas	Uppsala University, Sweden
Gerhard Schellhorn	University of Augsburg, Germany
Emil Sekerinski	McMaster University, Canada
Marjan Sirjani	Mälardalen University, Sweden
Volker Stolz	Western Norway University of Applied Sciences, Norway
Silvia Lizeth Tapia Tarifa	University of Oslo, Norway
Helen Treharne	University of Surrey, UK
Elena Troubitsyna	Åbo Akademi University, Finland
Frits W. Vaandrager	Radboud University, The Netherlands
Andrea Vandin	Sant'Anna School of Advanced Studies, Italy
Heike Wehrheim	University of Oldenburg, Germany
Anton Wijs	Eindhoven University of Technology, The Netherlands
Kirsten Winter	University of Queensland, Australia
Burkhart Wolff	Université Paris-Saclay, France
Naijun Zhan	Chinese Academy of Sciences, China

Artifact Evaluation Committee

Cedric Richter	University of Oldenburg, Germany
Pedro Ribeiro	University of York, UK
Felix Pauck	Paderborn University, Germany
Emilio Incerto	IMT School for Advanced Studies Lucca, Italy
Virgile Robles	CEA List, France
Yannic Noller	National University of Singapore, Singapore
Davide Basile	ISTI-CNR, Italy
Martin Tappler	Graz University of Technology, Austria
Bishoksan Kafle	University of Melbourne, Australia
Mathias Fleury	University of Freiburg, Germany
Danilo Pianini	University of Bologna, Italy
Sharar Ahmadi	University of Surrey, UK

PhD Symposium Program Committee

Wolfgang Ahrendt	Chalmers University of Technology, Sweden
Clare Dixon	University of Manchester, UK
Angelo Ferrando	University of Genova, Italy
Ivan Perez	National Institute of Aerospace and NASA, USA
Alexandra Mendes	University of Porto and INESC TEC, Portugal

Maike Schwammberger
Graeme Smith

University of Oldenburg, Germany
University of Queensland, Australia

Steering Committee

Erika Ábrahám	RWTH Aachen University, Germany
Wolfgang Ahrendt	Chalmers University of Technology, Sweden
Ferruccio Damiani	University of Turin, Italy
John Derrick	University of Sheffield, UK
Carlo A. Furia	Università della Svizzera italiana, Switzerland
Marieke Huisman	University of Twente, The Netherlands
Einar Broch Johnsen	University of Oslo, Norway
Luigia Petre	Åbo Akademi University, Finland
Nadia Polikarpova	University of California, San Diego, USA
Steve Schneider	University of Surrey, UK
Emil Sekerinski	McMaster University, Canada
Silvia Lizeth Tapia Tarifa	University of Oslo, Norway
Helen Treharne	University of Surrey, UK
Heike Wehrheim	University of Oldenburg, Germany
Kirsten Winter	University of Queensland, Australia

Local Organizers

Mohammad Rezaalipour	Università della Svizzera italiana, Switzerland
Diego Marcilio	Università della Svizzera italiana, Switzerland
Elisa Larghi	Università della Svizzera italiana, Switzerland
Roberto Minelli	Università della Svizzera italiana, Switzerland

Additional Reviewers

Sara Abbaspour Asadollah	Constantin Catalin Dragan	Violet Ka I Pun
Ole Jørgen Abusdal	Jannik Dunkelau	Cedric Richter
Sharar Ahmadi	Mamoun Filali-Amine	Justus Sagemüller
Christian Attiogbe	Paul Fiterău-Brosteau	Joshua Schmidt
Boutheina Bannour	Predrag Filipovikj	Arnab Sharma
Chinmayi Prabhu	Aditi Kabra	William Simmons
Baramashetru	Eduard Kamburjan	Marek Trtík
Nikola Benes	Paul Kobiálka	Fabian Vu
Lionel Blatter	Stefan Marksteiner	Shuling Wang
Jean-Paul Bodeveix	Hugo Musso Gualandi	Simon Wimmer
Zheng Cheng	Muhammad Osama	Hao Wu
Sadegh Dalvandi	Felix Pauck	Tengshun Yang
Crystal Chang Din	Valentin Perrelle	Bohua Zhan

Side Channel Secure Software (Abstract of Invited Talk)

Roderick Bloem 

University of Technology, Austria
roderick.bloem@iaik.tugraz.at

Abstract. We will present a method to analyze masked hardware or masked software for vulnerability to power side channel attacks. Masking is a technique to hide secrets by duplication and addition of randomness. We use the Fourier expansion of Boolean functions to find correlations between variables and secrets and we present an abstraction-refinement technique that reduces the search for correlations to the satisfiability of a formula in propositional logic. This technique allows us to find leaks in industrial-size circuits, while taking detailed timing aspects such as glitching into account.

Formal methods to analyze the power side channel security of software often take a simplistic view of the side-channel leakage that is incurred during a software execution. We take a detailed look at how software executes on a real processor, and specifically on the IBEX RISC-V CPU. Using our verification tool, we find vulnerabilities that are surprising on first glance. We present both modifications to harden a CPU against leaks and guidelines for writing software that can be proven not to leak any further information.

References

1. Bloem, R., Gros, H., Iusupov, R., Könighofer, B., Mangard, S., Winter, J.: Formal verification of masked hardware implementations in the presence of glitches. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10821, pp. 321–353. Springer (2018). https://doi.org/10.1007/978-3-319-78375-8_11
2. Gigerl, B., Hadzic, V., Primas, R., Mangard, S., Bloem, R.: Coco: co-design and co-verification of masked software implementations on CPUs. In: Bailey, M., Greenstadt, R. (eds.) 30th USENIX Security Symposium (USENIX Security 2021), August 11–13, 2021, pp. 1469–1468. USENIX Association (2021). <https://www.usenix.org/conference/usenixsecurity21/presentation/gigerl>
3. Hadzic, V., Bloem, R.: CocoAlma: a versatile masking verifier. In: Proceedings of the 21st Conference on Formal Methods in Computer Aided Design (FMCAD 2021), New Haven, CT, USA, October 19–22, 2021, pp. 1–10. IEEE (2021). https://doi.org/10.34727/2021/isbn.978-3-85448-046-4_9, <https://ieeexplore.ieee.org/document/9617707/>

Contents

Invited Presentations

- Verifying Autonomous Systems 3
Louise A. Dennis
- Empowering the Event-B Method Using External Theories 18
*Yamine Ait-Ameur, Guillaume Dupont, Ismail Mendil, Dominique Méry,
Marc Pantel, Peter Rivière, and Neeraj K. Singh*

Cooperative and Relational Verification

- Journal-First: Formal Modelling and Runtime Verification of Autonomous
Grasping for Active Debris Removal 39
*Marie Farrell, Nikos Mavrikis, Angelo Ferrando, Clare Dixon,
and Yang Gao*
- Formal Specification and Verification of JDK’s Identity Hash Map
Implementation 45
*Martin de Boer, Stijn de Gouw, Jonas Klamroth, Christian Jung,
Mattias Ulbrich, and Alexander Weigl*
- Reusing Predicate Precision in Value Analysis 63
Marie-Christine Jakobs
- Certified Verification of Relational Properties 86
Lionel Blatter, Nikolai Kosmatov, Virgile Prevosto, and Pascale Le Gall

B Method

- Reachability Analysis and Simulation for Hybridised Event-B Models 109
*Yamine Ait-Ameur, Sergiy Bogomolov, Guillaume Dupont,
Neeraj Kumar Singh, and Paulius Stankaitis*
- Operation Caching and State Compression for Model Checking
of High-Level Models: How to Have Your Cake and Eat It 129
Michael Leuschel

Time

- Conservative Time Discretization: A Comparative Study 149
Marcelo Forets and Christian Schilling

Untangling the Graphs of Timed Automata to Decrease the Number of Clocks	168
<i>Neda Saeedloei and Feliks Kluzniak</i>	

Probability

Probabilistic Model Checking of BPMN Processes at Runtime	191
<i>Yliès Falcone, Gwen Salaün, and Ahang Zuo</i>	
HyperPCTL Model Checking by Probabilistic Decomposition.	209
<i>Eshita Zaman, Gianfranco Ciardo, Erika Abraham, and Borzoo Bonakdarpour</i>	

Learning and Synthesis

Learning Finite State Models from Recurrent Neural Networks	229
<i>Edi Muškardin, Bernhard K. Aichernig, Ingo Pill, and Martin Tappler</i>	
Kaki: Concurrent Update Synthesis for Regular Policies via Petri Games	249
<i>Nicklas S. Johansen, Lasse B. Kær, Andreas L. Madsen, Kristian Ø. Nielsen, Jiří Srba, and Rasmus G. Tollund</i>	

Security

Verified Password Generation from Password Composition Policies	271
<i>Miguel Grilo, João Campos, João F. Ferreira, José Bacelar Almeida, and Alexandra Mendes</i>	
A Policy Language to Capture Compliance of Data Protection Requirements	289
<i>Chinmayi Prabhu Baramashetru, Silvia Lizeth Tapia Tarifa, Olaf Owe, and Nils Gruschka</i>	

Static Analysis and Testing

Extending Data Flow Coverage to Test Constraint Refinements	313
<i>Alexander Kolchin and Stepan Potiyenko</i>	
Scalable Typestate Analysis for Low-Latency Environments	322
<i>Alen Arslanagić, Pavle Subotić, and Jorge A. Pérez</i>	

PhD Symposium Presentations

Studying Users' Willingness to Use a Formally Verified Password Manager	343
<i>Carolina Carreira</i>	

Modeling Explanations in Autonomous Vehicles. 347
Akhila Bairy

A Requirements-Driven Methodology: Formal Modelling and Verification
of an Aircraft Engine Controller 352
Oisín Sheridan, Rosemary Monahan, and Matt Luckcuck

A Dialogue Interface for Low Code Program Evolution. 357
Luís Carvalho

Simple Dependent Types for OSTRICH. 361
Joana Parreira

SNITCH: A Platform for Information Flow Control. 365
Eduardo Geraldo

Machine-Assisted Proofs for Institutions in Coq 369
Conor Reynolds and Rosemary Monahan

Author Index 373