

**VIJAY GANESH**  
**Associate Professor, University of Waterloo, Canada**

200 University Ave. West, DC 2530  
University of Waterloo, ECE and CS  
Waterloo, Ontario, Canada N2L 3G1

Phone: +1-519-888-4567 ext. 32866  
Email: [vganesh@uwaterloo.ca](mailto:vganesh@uwaterloo.ca)  
Web: <https://ece.uwaterloo.ca/~vganesh>

**EDUCATION**

---

<b>Degree</b>	<b>Institution</b>	<b>Graduation Date</b>
PhD, Computer Science	<b>Stanford University</b> , CA, USA	Sep 2007
MS, Electrical Engineering	<b>Stanford University</b> , CA, USA	Jun 2000
B-Tech, Electronics and Communication	<b>College of Engineering, Trivandrum</b> , Kerala, India	Nov 1994

**FULL-TIME ACADEMIC APPOINTMENTS**

---

<b>Research Position</b>	<b>Institution</b>	<b>Dates</b>
Associate Professor (with tenure)	ECE and CS (cross-appointed), <b>University of Waterloo</b> , Ontario, Canada	Jul 2018 – present
Assistant Professor	ECE and CS (cross-appointed), <b>University of Waterloo</b> , Ontario, Canada	Sep 2012 – Jun 2018
Research Scientist	<b>Massachusetts Institute of Technology</b> , Cambridge, MA, USA	Oct 2007 – Sep 2012

**VISITING ACADEMIC APPOINTMENTS**

---

<b>Research Position</b>	<b>Institution</b>	<b>Dates</b>
Visiting Professor	Computer Science, <b>Indian Institute of Technology</b> , Bombay, India	Jan 2020 – Dec 2021
Long-term Visiting Researcher	<b>Simons Institute</b> for Theory of Computing, <b>Berkeley</b> , CA, USA	Jan 2021 – May 2021
Visiting Professor	Computer Science, <b>University of Toronto</b> , Ontario, Canada	Sep 2019 – Feb 2020 Jan 2016 – Mar 2016
Visiting Professor	Chebyshev Labs, <b>St. Petersburg State University</b> , St. Petersburg, Russia	Apr 2016 – Jun 2016

**RESEARCH INTERESTS**

---

Boolean SAT and SMT Solvers, Machine Learning (ML) for Solvers and Solvers for ML  
Testing, Analysis, Verification, and Security of Software and AI Systems  
Proof Complexity of Solvers, Theorem Provers, and Formal Methods  
Application of Solvers in Engineering, Mathematics, and Physics  
Mathematical Logic and Foundations of Mathematics

## AWARDS, HONORS, AND DISTINCTIONS

---

The primary focus of my research is the theory and practice of mathematical reasoning algorithms (aka, SAT/SMT solvers), and their applications in software engineering, security, formal methods, mathematics, and physics. In this context, I have received **more than 25 awards, medals, and distinctions** of various kinds for my research, including an **ACM ISSTA Impact Paper Award 2019 (best paper in 10 years)**, won two gold medals at the SAT 2016 competition and two silver medals at the SAT 2017 competition, an Early Researcher Award in 2016, an **ACM Test of Time Award at CCS 2016 (best paper in 10 years)**, two Google Faculty Research Awards in 2013 and 2011, a citation for **10-year most-influential papers at the DATE conference in 2008 (best paper in 10 years)**, and more than 10 best paper awards/honors of various kinds. A few of these awards and distinctions are listed below. The rest can be found on my [website](#).

1. **ACM ISSTA IMPACT Paper Award 2019 (Best Paper in 10 Years @ ISSTA conference)**
2. Won two silver medals at the [SAT competition 2017](#)
3. **ACM CCS Test of Time Award 2016 (Best Paper in 10 Years @ ACM CCS conference)**
4. [Outstanding Paper at the Annual Computer Security Applications Conference \(ACSAC\) 2016](#)
5. [Early Researcher Award \(ERA\) 2016, Ontario, Canada](#)
6. Won two gold medals at the [SAT competition 2016](#)
7. [IBM Faculty Award 2015](#)
8. [MathCheck](#) paper selected as among Best Papers at CADE 2015, Berlin, Germany
9. [Z3str2 String Solver](#) paper selected as among Best Papers at CAV 2015, San Francisco, USA
10. Best Paper Award at the Software Product Lines Conference (SPLC) 2015
11. [Google Faculty Research Award 2013](#) (Only 15 winners worldwide in software engineering)
12. [Heidelberg Laureate Forum Invitee 2013](#) (Highly selective conference where young researchers are invited to meet with Fields, Turing, and Abel prize winners. My [blog post](#) on the event.)
13. [Google Faculty Research Award 2011](#) (Only 12 winners worldwide in software engineering)
14. [ACM SIGSOFT Distinguished Paper Award at ISSTA 2009](#)
15. **Ten-year most influential paper at DATE 2008 (Best Paper in 10 Years @ ACM/IEEE DATE conference)**

## RESEARCH FUNDING HISTORY

Funding Program	Project Title	PI	Agency	Funds CAD (My share)	Duration
NSERC Discovery	Machine Learning and Solvers: The Next Frontier	Vijay Ganesh	NSERC	\$205K (100%)	Apr 2020-Apr 2025
Amazon AWS	Amazon AWS for Automated Reasoning	Vijay Ganesh	Amazon Inc.	\$193K (100%)	Jan 2019-Jan 2021
Ripple	Ripple Faculty Fellow: Security of Smart Contracts	Vijay Ganesh	Ripple Inc.	\$120K (100%)	Jan 2019-Jan 2023
Amazon	String Solvers for Security	Vijay Ganesh	Amazon Inc.	\$187K (100%)	Jan 2018-Jan2020
NSERC Discovery Extension	Next-generation Constraint Solvers for Software Engineering and Security	Vijay Ganesh	NSERC	\$25K (100%)	Apr 2018-Mar 2019
NSERC CRD 2017 (Co-PI)	Accelerating multi-objective combinatorial optimizations via GPUs for Cyber-Physical Systems Design	Krzysztof Czarnecki	NSERC	\$150K (25%)	Jan 2017 - Dec 2018
<a href="#">Early Researcher Award 2016</a>	Solvers for Security via a Combination of Machine Learning and Deduction	Vijay Ganesh	Ontario	\$150K (100%)	Jun 2016 - Jun 2021
<a href="#">IBM Faculty Award 2015</a>	String Solvers for Mobile and Cloud Security	Vijay Ganesh	IBM	\$7.5K (100%)	Dec 2015 - Mar 2017
NSERC Create 2015 (Co-PI)	Product-Line Engineering for Cyber-Physical Systems	Krzysztof Czarnecki	NSERC	\$1,650K (8%)	Apr 2015 - Mar 2021
NSERC Discovery 2013	Next-generation Constraint Solvers for Software Engineering and Security	Vijay Ganesh	NSERC	\$125K (100%)	Apr 2013 - Mar 2018
<a href="#">Google Faculty Award 2013</a>	From Functional Regressions to Security Testing	Vijay Ganesh	Google	\$15K (100%)	Oct 2013 - Oct 2016
Waterloo ECE Starter 2012	University of Waterloo ECE Departmental Seed Funding for Junior Faculty	Vijay Ganesh	ECE, Waterloo	\$125K (100%)	Sep 2012 - present
<a href="#">Google Faculty Award 2011</a>	Constraint Solvers for Security Testing	Vijay Ganesh	Google	\$60K (100%)	Sep 2011 - Sep 2016
NSF Grant 0905244 2009 (Co-PI)	Exposing and Eliminating Errors at Component Boundaries	Martin Rinard	NSF, USA	\$682K (33%)	Oct 2009 - Sep 2012
<b>Total award**</b>				<b>\$3.7M</b>	

\*\* All funds are in Canadian dollars. My share of the total is approx. \$2 million Canadian dollars.

Following are some of my most significant practical and theoretical research contributions in the context of theory, practice, and applications of SAT and SMT solvers. Briefly, I describe here the use of ML techniques in solver algorithms, applications of solvers in software engineering (testing, analysis, verification, and synthesis), security, AI, and mathematics, as well as complexity-theoretic results in the context of first-order theories over strings and upper/lower bounds for solver algorithms.

### Important Practical Results

#### 1. Machine Learning for Logic: ML-based Solvers and Provers (2014–present)

SAT and SMT solvers are mathematical reasoning algorithms aimed at solving the **satisfiability problem** for Boolean logic and first-order theories respectively. The Boolean satisfiability (or SAT) problem is rightly considered one of the most important problems in computer science and mathematics. Even though the SAT problem has been shown to be NP-complete, and is considered to be intractable, modern conflict-driven clause-learning (CDCL) SAT solvers are capable of solving real-world formulas with tens of millions of variables and clauses in them. As a consequence, they have found wide applicability in diverse areas such as software engineering, security, AI, mathematics, and physics.

One of the most important questions in SAT research is the following: **“why are solvers so efficient, despite the fact that the SAT problem is NP-complete?”**

In my attempt to answer the above question, my collaborators and I made a set of crucial discoveries:

It has been known that solvers can be best understood as algorithms that implement proof systems (e.g., resolution). However, until recently, solver implementations used ad-hoc methods to implement these proof systems. By contrast, we showed that solver design can be dramatically improved in terms of efficiency, extensibility and quality if solver optimization heuristics (aimed at optimally sequencing and selecting proof rules) are implemented using both online and offline machine learning techniques. The underlying reason for this is that solvers produce copious amount of data as they perform their analysis and proof search, and this data can be leveraged using ML techniques to dynamically optimize the solver’s performance.

**This idea that SAT solvers are implementations of proof rules (logic) and ML optimization heuristics underpins the design of our award-winning SAT solver, MapleSAT.** A version of this solver won two gold medals and two silver medals at the annual SAT competition in 2016 and 2017 respectively, and has deeply impacted the field of solver design. Other researchers have adopted and adapted ideas from the design of the MapleSAT solver for their own solver algorithms.

Second, theorists and practitioners have long held the view that SAT solvers work well for real-world instances because of their inherent structure that can be described parametrically and used to prove upper/lower parameterized complexity-theoretic bounds. While many parameters have been proposed, they all fail in some way or the other to appropriately describe this phenomenon of solver efficiency. **After extensive empirical work, my collaborators and I have identified a set of parameters, namely, hierarchical community structure and mergeability, that can be shown to empirically explain why solvers are so efficient for real-world instances. Further, we have results that suggest that these parameters may finally help establish parameterized complexity-theoretic upper bounds that explain why SAT solvers are efficient.**

#### 2. String solvers for software engineering and security (2009–present)

The problem of designing efficient string solving algorithms is widely recognized as one of the most difficult in the context of SMT solvers. These solvers are a particularly important class of tools in the context of computer security. Since 2009, I have co-designed a series of string solving algorithms that are efficient for

many security applications, culminating in the co-design and implementation of the Z3str3 string solver. **My decade-long work on the theory and practice of string solvers led to an ACM IMPACT Paper Award at ISSA 2019.**

### 3. STP Solver for scalable symbolic analysis (2005–2012)

One of my most impactful practical result is the design and implementation of the STP bit-vector and array solver that **played an important role in the development of scalable symbolic execution, widely considered a breakthrough in software engineering and security.** The STP solver’s success can be credited to several abstraction-refinement style algorithms that I came up with for deciding bit-vector and array formulas. These algorithms have stood the test of time and continue to be used and extended to novel settings. STP has been used to find thousands of bugs in many critical pieces of software including Debian Linux and is currently used in many companies to do automated test case generation. This work led to an **ACM Test of Time Award at the CCS 2016 conference.**

## Important Theoretical Results

### 1. Theories over strings (2009–present)

I have done extensive work in the context of decidability and complexity-theoretic questions for theories over strings. Specifically, in 2017, I proved that the quantifier-free theory of string equations, length function, and string-integer conversion is undecidable, and in 2012, I proved that the theory of string equations with a single quantifier-alternation is undecidable. Further, my collaborators and I proved several complexity results for various fragments and extensions of this theory. For example, in 2018 we established the PSPACE-completeness of the quantifier-free theory of simple regular expressions, arithmetic over string length function, and concatenation of string terms.

### 2. MathCheck SAT+CAS combination to counterexample math conjectures (2014-present)

Since 2015, my students and I have been developing a tool that combines a SAT solver and a computer algebra system (CAS) that we have used to finitely verify several open conjectures. For example, in 2016 we settled an important question in combinatorial mathematics, namely, “what is smallest counterexample to the Williamson construction for the Hadamard conjecture”, a problem that had been open since 1944.

### 3. Proof complexity of SAT and SMT solvers (2016-present)

In 2018, my collaborators and I proved some of the first results on proof complexity of SMT solvers. Proof complexity gives us unique insights into formal verification algorithms since they are essentially proof systems. We can gain deep understanding into why solvers are efficient via parameterized proof complexity. More recently, we showed that CDCL SAT solvers are polynomially equivalent to merge resolution.

## INDUSTRIAL EXPERIENCE

---

Oct 2017 – Jun 2019, Founding Advisor, **Quantstamp and Blockchain Development Labs (BDL)**, Toronto, Ontario, Canada: Advisor on security analysis methods

May 1999 - Aug 1999, Research Intern, SRI International, Menlo Park, CA, USA: Designed and implemented a slicing tool for the Java programming language

Feb 1996 - Sep 1997, Software Engineer, Texas Instruments (India) Ltd, Bangalore, India: Designed and implemented instruction set simulators for TI’s C54x DSP chips

Nov 1994 - Dec 1995, Software Engineer, Larsen & Toubro (India) Ltd, Mumbai, India: Designed and implemented software for industrial programmable logic controllers

## PUBLICATION METRICS

---

I have used the highly reputed conference ranking website [CORE](#), a ranking by consortium of Australian academics, to rank venues where my most important papers have been published.

Topic	Venue ID	Full Name of Conference Venue	CORE	Number of papers
Artificial Intelligence	AAAI	Association for Advancement of Artificial Intelligence	A*	7
Formal Methods	CAV	International Conference on Computer Aided Verification	A*	6
Artificial Intelligence	IJCAI	International Joint Conference on Artificial Intelligence	A*	3
Software Engineering	ICSE	International Conference on Software Engineering	A*	3
Computer Security	CCS	International Conference on Computer and Communications Security	A*	2
Artificial Intelligence	ICML	International Conference on Machine Learning	A*	1
Automated Reasoning	SAT	Theory and Application of Satisfiability Testing	A	9
Automated Reasoning	CP	Principles and Practice of Constraint Programming	A	4
Software Engineering	ISSTA	International Symposium on Software Testing and Analysis	A	2

## PUBLICATIONS

---

The names of the authors listed below are presented in order of their contributions, with the highest contributor as the first author. The names of my students and postdocs are marked with a '\*'. You can also find my publications on [DBLP](#), as well as on Google Scholar in [highest-cited first](#) order.

### BOOK CHAPTERS

- B1. **Vijay Ganesh** and Moshe Vardi. 2020. **On the Unreasonable Effectiveness of SAT Solvers**. In Tim Roughgarden (Ed.), **Beyond the Worst-case Analysis of Algorithms**. Cambridge University Press (CUP). pp. 547-567.

### Ph.D. THESIS, STANFORD UNIVERSITY, CA, USA

- T1. **Vijay Ganesh**. PhD Thesis Title: Decision Procedures for Bit-vectors, Arrays, and Integers. Stanford University, Stanford, CA, USA. September 2007. Advisor: David L. Dill.

### PEER-REVIEWED CONFERENCE PUBLICATIONS

- C1. Joseph Scott\*, Aina Niemetz, Mathias Preiner, Saeed Nejati\*, and **Vijay Ganesh**. MachSMT: A Machine Learning-based Algorithm Selector for SMT Solvers. In the Proceedings of the 27<sup>th</sup> International Conference on Tools & Algorithms for the Construction & Analysis of Systems (TACAS 2021), Virtual Conference.

- C2. Laura Graves\*, Vineel Nagisetty\*, and **Vijay Ganesh**. Amnesiac Machine Learning. Accepted at the 35<sup>th</sup> AAAI Conference on Artificial Intelligence (**AAAI 2021**).
- C3. Dhananjay Ashok, Joseph Scott\*, Maysum Panju, Sebastian Wetzel, and **Vijay Ganesh**. Logic-Guided Genetic Algorithms. Accepted at the 35<sup>th</sup> AAAI Conference on Artificial Intelligence (**AAAI 2021**).
- C4. Curtis Bright\*, Kevin K. H. Cheung, Brett Stevens, Ilias S. Kotsireas, and **Vijay Ganesh**. A SAT-based Resolution of Lam’s Problem. Accepted at the 35<sup>th</sup> AAAI Conference on Artificial Intelligence (**AAAI 2021**).
- C5. Saeed Nejati\*, Ludovic Le Frioux, and **Vijay Ganesh**. A Machine Learning-based Splitting Heuristic for Divide-and-Conquer Solvers. In the Proceedings of the 26<sup>th</sup> International Conference on the Principles and Practices of Constraint Programming (**CP 2020**). Virtual Conference (originally at Louvain-la-Neuve, Belgium), Sep 7 - Sep 11, 2020.
- C6. Haonan Duan, Saeed Nejati\*, George Trimponias, Pascal Poupart, and **Vijay Ganesh**. Online Bayesian Moment Matching based SAT Solver Heuristics. International Conference on Machine Learning (**ICML 2020**). Virtual Conference (originally at Vienna, Austria), Jul 12 – Jul 18, 2020.
- C7. Curtis Bright\*, Kevin K. H. Cheung, Brett Stevens, Ilias S. Kotsireas, and **Vijay Ganesh**. Unsatisfiability Proofs for Weight 16 Codewords in Lam’s Problem. In the Proceedings of the 29<sup>th</sup> International Joint Conference on Artificial Intelligence (**IJCAI 2020**). Virtual Conference (originally at Yokohama, Japan in July 2020), Jan 7 – Jan 15, 2021.
- C8. Joseph Scott\*, Federico Mora, and **Vijay Ganesh**. BanditFuzz: A Reinforcement-Learning based Performance Fuzzer for SMT Solvers. In the Proceedings of the 12<sup>th</sup> Working Conference on Verified Software: Theories, Tools, and Experiments (**VSTTE 2020**). Virtual Conference (originally at Los Angeles, USA), July 20-21, 2020.
- C9. Vincent Vallade, Ludovic Le Frioux, Souheib Baarir, Julien Sopena, **Vijay Ganesh**, and Fabrice Kordon. Community and LBD-based Clause Sharing Policy for Parallel SAT Solving. In the Proceedings of the 23<sup>rd</sup> International Conference on Theory and Applications of Satisfiability Testing (**SAT 2020**). Virtual Conference (originally at Alghero, Italy), Jul 3 – Jul 10, 2020.
- C10. Chunxiao Li\*, Noah Fleming, Marc Vinyals, Toniann Pitassi, and **Vijay Ganesh**. Towards a Complexity-theoretic Understanding of Restarts in SAT Solvers. In the Proceedings of the 23<sup>rd</sup> International Conference on Theory and Applications of Satisfiability Testing (**SAT 2020**). Virtual Conference (originally at Alghero, Italy), Jul 3 – Jul 10, 2020.
- C11. Joseph Scott\*, Maysum Panju, and **Vijay Ganesh**. Logic Guided Machine Learning. In the Proceedings of the 34<sup>th</sup> AAAI Conference on Artificial Intelligence (**AAAI 2020**), New York City, USA, Feb 7 – Feb 12, 2020.
- C12. Curtis Bright\*, Ilias Kotsireas, and **Vijay Ganesh**. SAT Solvers and Computer Algebra Systems: A Powerful Combination for Mathematics. In the Proceedings of the 29<sup>th</sup> Annual International Conference on Computer Science and Software Engineering (**CASCON 2019**), Toronto, Canada, Nov 4, 2019.
- C13. Saeed Nejati\* and **Vijay Ganesh**. CDCL(Crypto) SAT Solvers for Cryptanalysis. In the Proceedings of the 29<sup>th</sup> Annual International Conference on Computer Science and Software Engineering (**CASCON 2019**), Toronto, Canada, Nov 4, 2019.



- C14. William Zhang\*, Sebastian Banescu, Steven Stewart, Leonardo Passos, and **Vijay Ganesh**. M-Pro: Combining Static and Symbolic Analysis for Scalable Testing of Smart Contracts. In the Proceedings of the 30<sup>th</sup> International Symposium on Software Reliability Engineering (**ISSRE 2019**), Berlin, Germany, Oct 28 – 31, 2019.
- C15. Reza Babae\*, **Vijay Ganesh**, and Sean Edwards. Accelerated Learning of Predictive Runtime Monitors for Rare Failure. In the Proceedings of the 19<sup>th</sup> International Conference on Runtime Verification (**RV 2019**), Porto, Portugal, October 8-11, 2019.
- C16. Curtis Bright\*, Jeurgen Gerhard, Ilias Kotsireas, and **Vijay Ganesh**. Effective Problem-Solving using SAT Solvers. In the Proceedings of the Annual Maple Conference (**Maple 2019**), Waterloo, Ontario, Canada, Oct 15 – Oct 17, 2019.
- C17. Hari Govind\*, Yakir Vizel, **Vijay Ganesh**, and Arie Gurfinkel. Interpolating Strong Induction. In the Proceedings of the 31<sup>st</sup> International Conference on Computer Aided Verification (**CAV 2019**), New York City, New York, USA, July 15-18, 2019.
- C18. Adam Kiezun, Philip J. Guo, Pieter Hooimeijer, Michael D. Ernst, and **Vijay Ganesh**. Theory and Practice of String Solvers. In the Proceedings of the 28<sup>th</sup> ACM SIGSOFT International Symposium on Software Testing and Analysis (**ISSTA 2019**), Beijing, China, July 15-19, 2019.  
[ACM IMPACT Paper Award at ISSTA 2019](#)
- C19. Curtis Bright\*, Dragomir Djokovic, Ilias Kotsireas, and **Vijay Ganesh**. A SAT+CAS Approach to Finding Good Matrices: Examples and Counterexamples. In the Proceedings of the 33<sup>rd</sup> AAAI Conference on Artificial Intelligence (**AAAI 2019**), Honolulu, Hawaii, USA, Jan 27 – Feb 1, 2019.
- C20. Joel Day, Paul He\*, Florin Manea, Dirk Nowotka, and **Vijay Ganesh**. The Satisfiability of Word Equations: Decidable and Undecidable Theories. In the Proceedings of the 12<sup>th</sup> International Conference on Reachability Problems (**RP 2018**), Marseille, France, September 24-26, 2018.
- C21. Saeed Nejati\*, Jan Horacek, Catherine Gebotys, and **Vijay Ganesh**. Algebraic Fault Attacks on SHA Hash Functions using Programmatic SAT Solvers. In the Proceedings of the 24<sup>th</sup> International Conference on the Principles and Practices of Constraint Programming (**CP 2018**), Lille, France, August 26-31, 2018.
- C22. Edward Zulkoski\*, Ruben Martins, Christoph M. Wintersteiger, Robert Robere, Jia Hui Liang\*, Krzysztof Czarnecki and **Vijay Ganesh**. The Effect of Structural Measures and Merges on SAT Solver Performance. In the Proceedings of the 24<sup>th</sup> International Conference on the Principles and Practices of Constraint Programming (**CP 2018**), Lille, France, August 26-31, 2018.
- C23. Edward Zulkoski\*, Ruben Martins, Christoph M. Wintersteiger, Jia Hui Liang\*, Krzysztof Czarnecki and **Vijay Ganesh**. Learning Sensitive Backdoors with Restarts. In the Proceedings of the 24<sup>th</sup> International Conference on the Principles and Practices of Constraint Programming (**CP 2018**), Lille, France, August 26-31, 2018.
- C24. Curtis Bright\*, Albert Heinle, Ilias Kotsireas, and **Vijay Ganesh**. Enumeration of Complex Golay Pairs via Programmatic SAT. In the Proceedings of 43<sup>rd</sup> International Symposium of Symbolic and Algebraic Computation (**ISSAC 2018**), New York City, New York, USA, July 16-19, 2018.
- C25. Jia Hui Liang\*, Hari Govind\*, Pascal Poupart, Krzysztof Czarnecki, and **Vijay Ganesh**. An Empirical Study of Branching Heuristics through the Lens of Global Learning Rate. In the Proceedings of the 27<sup>th</sup> International Joint Conference on Artificial Intelligence (**IJCAI 2018**), Stockholm, Sweden, July 13-19, 2018.  
[IJCAI 'Sister Conference Best Paper Track' Invited Paper 2018](#)



- C26. Robert Robere, Antonina Kolkolova, and **Vijay Ganesh**. The Proof Complexity of SMT Solvers. In the Proceedings of the 30<sup>th</sup> International Conference on Computer Aided Verification (**CAV 2018**), Oxford, United Kingdom, July 14-17, 2018.
- C27. Dmitry Blotsky\*, Federico Mora, Murphy Berzish\*, Yunhui Zheng, Ifaz Kabir, and **Vijay Ganesh**. StringFuzz: A Fuzzer for String Solvers. In the Proceedings of the 30<sup>th</sup> International Conference on Computer Aided Verification (**CAV 2018**), Oxford, United Kingdom, July 14-17, 2018.
- C28. Jia Hui Liang\*, Chanseok Oh, Minu Mathews, Ciza Thomas, Chunxiao Li, and **Vijay Ganesh**. A Machine Learning based Restart Policy for CDCL SAT Solvers. In the Proceedings of the 21<sup>st</sup> International Conference on Theory and Applications of Satisfiability Testing (**SAT 2018**), Oxford, United Kingdom, July 9-12, 2018.
- C29. Curtis Bright\*, Ilias Kotsireas, and **Vijay Ganesh**. A SAT+CAS Method for Enumerating Williamson Matrices of Even Orders. In the Proceedings of the 32<sup>nd</sup> AAAI Conference on Artificial Intelligence (**AAAI 2018**), New Orleans, Louisiana, USA, February 2-7, 2018.
- C30. Jia Hui Liang\*, Hari Govind\*, Pascal Poupart, Krzysztof Czarnecki, and **Vijay Ganesh**. An Empirical Study of Branching Heuristics through the Lens of Global Learning Rate. In the Proceedings of the 20<sup>th</sup> International Conference on Theory and Application of Satisfiability Testing (**SAT 2017**), Melbourne, Australia, Aug 28 – Sep 1, 2017. [Among Top Three Best Papers @ SAT 2017](#)
- C31. Saeed Nejati\*, Zack Newsham\*, Joe Scott\*, Jia Hui Liang\*, Catherine Gebotys, Pascal Poupart, and **Vijay Ganesh**. A Propagation Rate based Splitting Heuristic for Divide-and-Conquer Solvers. In the Proceedings of the 20<sup>th</sup> International Conference on Theory and Application of Satisfiability Testing (**SAT 2017**), Melbourne, Australia, Aug 28 – Sep 1, 2017.
- C32. Murphy Berzish\*, Yunhui Zheng, and **Vijay Ganesh**. Z3str3: A String Solver with Theory-Aware Branching. In the Proceedings of the 17<sup>th</sup> Formal Methods in Computer Aided Design Conference (**FMCAD 2017**), Vienna, Austria, Oct 2-6, 2017.
- C33. Saeed Nejati\*, Jia Hui Liang\*, **Vijay Ganesh**, Catherine Gebotys, and Krzysztof Czarnecki. Adaptive Restart and CEGAR-based Solver for Inverting Cryptographic Hash Functions. In the Proceedings of the 9<sup>th</sup> Working Conference on Verified Software: Theories, Tools, and Experiments (**VSTTE 2017**), Heidelberg, Germany, July 22-23, 2017.
- C34. Sanu Subramanian\*, Murphy Berzish\*, **Vijay Ganesh**, Omer Tripp. A Solver for a Theory of Bit-vectors and Strings. In the Proceedings of 39<sup>th</sup> International Conference on Software Engineering (**ICSE 2017**), Companion Vol., Buenos Aires, Argentina, May 20-28, 2017. Pages 124-126.
- C35. Martin Ochoa, Sebastian Banescu, Cynthia Disenfeld, Gilles Barthe, and **Vijay Ganesh**. Reasoning about Probabilistic Defense Mechanisms against Remote Attacks. In the Proceedings of 2<sup>nd</sup> IEEE European Symposium on Security and Privacy (**EuroSP 2017**), Paris, France, Apr 26-28, 2017.
- C36. Sebastian Banescu, Zack Newsham\*, **Vijay Ganesh**, Christian Collberg, and Alexander Pretchner. Code Obfuscation Against Symbolic Execution Attacks. In the Proceedings of the 32<sup>nd</sup> Annual Computer Security Applications Conference (**ACSAC 2016**), Los Angeles, USA, Dec 5-9, 2016. Pages 189-200.  
[Outstanding Paper Award @ ACSAC 2016](#)
- C37. Murphy Berzish\*, Asif Khan, Atulan Zaman, **Vijay Ganesh**, and Derek Rayside. Manifold: An SMT-Based Declarative Language for Electronic and Microfluidic Design Synthesis. Proceedings of the 26<sup>th</sup> International Conference on Computer Science and Software Engineering Conference (**CASCON 2016**), Toronto, Canada, Oct 31-Nov 2, 2016. Pages 188-193.

- C38. Riyad Parvez\*, **Vijay Ganesh**, Glenn Wurster, Joe Kirwin, and Paul Ward. Combining Static Analysis and Targeted Symbolic Execution for Scalable Bug-finding in Application Binaries. Proceedings of the 26<sup>th</sup> International Conference on Computer Science and Software Engineering Conference (**CASCON 2016**), Toronto, Canada, Oct 31-Nov 2, 2016. Pages 116-127.
- C39. Curtis Bright\*, **Vijay Ganesh**, Albert Heinle, Ilias Kotsireas, Saeed Nejati\*, and Krzysztof Czarnecki. MathCheck2: A SAT+CAS Verifier for Combinatorial Conjectures. In the Proceedings of the 18<sup>th</sup> International Conference on Computer Algebra in Scientific Computing (**CASC 2016**), Bucharest, Romania, Sep 19-23, 2016. Pages 117-133. [Symbolic Computation + Constraint Solving Track Invited Paper 2016](#)
- C40. Ed Zulkoski\*, **Vijay Ganesh**, and Krzysztof Czarnecki. MathCheck: A Math Assistant based on a Combination of Computer Algebra Systems and SAT Solvers. In the Proceedings of the 25<sup>th</sup> International Joint Conference on Artificial Intelligence (**IJCAI 2016**), New York, USA, July 9-15, 2016. Pages 4228-4223. [IJCAI 'Sister Conference Best Paper Track' Invited Paper 2016](#)
- C41. Steven Stewart, Derek Rayside, **Vijay Ganesh**, and Krzysztof Czarnecki. Accelerating the General Simplex Procedure for Linear Real Arithmetic via GPUs. In the Proceedings of the 8<sup>th</sup> Working Conference on Verified Software: Theories, Tools, and Experiments (**VSTTE 2016**), Toronto, Canada, July 17-18, 2016. Pages 129-138.
- C42. Jia Hui Liang\*, **Vijay Ganesh**, Pascal Poupart, and Krzysztof Czarnecki. Learning Rate Based Branching Heuristic for SAT Solvers. In the Proceedings of the 19<sup>th</sup> International Conference on Theory and Applications of Satisfiability Testing (**SAT 2016**), July 5, 2016. Pages: 123-140.
- C43. Jia Hui Liang\*, **Vijay Ganesh**, Pascal Poupart, and Krzysztof Czarnecki. Exponential Recency Weighted Average Branching Heuristic for SAT Solvers. Proceedings of the 30<sup>th</sup> AAAI Conference on Artificial Intelligence (**AAAI 2016**), Tuscon, Arizona, USA, February 12, 2016. Pages 3434-3440.
- C44. Jia Hui Liang\*, **Vijay Ganesh**, Ed Zulkoski\*, Atulan Zaman, and Krzysztof Czarnecki. Understanding VSIDS Branching Heuristic in Conflict-Driven Clause-Learning SAT Solvers. In Proceedings of the 11<sup>th</sup> International Haifa Verification Conference (**HVC 2015**), Haifa, Israel, Nov 17-19, 2015. Pages 225-241
- C45. Zack Newsham\*, William Lindsay\*, Jian Hui Liang\*, **Vijay Ganesh**, Sebastian Fischmeister, and Krzysztof Czarnecki. SATGraf: Visualising the Evolution of SAT Formula Structure in Solvers. In the Proceedings of the 18<sup>th</sup> International Conference on Satisfiability Testing (**SAT 2015**), Austin, USA, Sep 24-27, 2015. Pages 62-70.
- C46. Ed Zulkoski\*, **Vijay Ganesh**, and Krzysztof Czarnecki. MathCheck: A Math Assistant via a Combination of Computer Algebra Systems and SAT Solvers. In Proceedings of the 25<sup>th</sup> International Conference on Automated Deduction (**CADE 2015**), Berlin, Germany, Aug 1-7, 2015. pages 607-622. [Paper selected for Journal of Automated Reasoning Special Issue on Best Papers at CADE'15](#)
- C47. Yunhui Zheng, **Vijay Ganesh**, Sanu Subramanian\*, Omer Tripp, Julian Dolby and Xiangyu Zhang. Effective Search-space Pruning for Solvers of String Equations, Regular Expressions and Length Constraints. In Proceedings of the 27<sup>th</sup> International Conference on Computer-aided Verification (**CAV 2015**), San Francisco, July 20-24, 2015. Pages 235-254. [Paper selected for Formal Methods for System Design Special Issue on Best Papers at CAV'15](#)
- C48. Jia Hui Liang\*, **Vijay Ganesh**, Venkatesh Raman, and Krzysztof Czarnecki. Why SAT-based Analysis of Large Real-world Feature Models is Easy. In Proceedings of 19<sup>th</sup> International Software Product Line Conference (**SPLC 2015**), Nashville, Tennessee, USA, July 20-24, 2015. Pages 91-100. [Best paper award at SPLC 2015](#)

- C49. Zack Newsham\*, **Vijay Ganesh**, Gilles Audemard, Sebastian Fischmeister and Laurent Simon. The Impact of Community Structure on SAT Solver Performance. In the Proceedings of the 17<sup>th</sup> International Conference on Theory and Application of Satisfiability Testing (**SAT 2014**), Vienna, Austria, July 14-17, 2014. Pages 252-268. [Best student paper award at SAT 2014](#)
- C50. Yunhui Zheng, Xiangyu Zhang and **Vijay Ganesh**. Z3-str: A Z3-based String Solver for Web Application Analysis. In Proceedings of 9<sup>th</sup> Joint Meeting on Foundations of Software Engineering (**FSE 2013**), St. Petersburg, Russia, August 18-26, 2013. Pages 114-124. Acceptance Rate 20%
- C51. **Vijay Ganesh**, Mia Minnes, Armando Solar-Lezama and Martin C. Rinard. Word Equations with Length Constraints: What's Decidable? In the Proceedings of the 8<sup>th</sup> Haifa Verification Conference (**HVC 2012**), Haifa, Israel, Nov 2012. Pages 209-226.
- C52. Fan Long, **Vijay Ganesh**, Michael Carbin, Stelios Sidroglou and Martin C. Rinard. Automatic Input Rectification. In the Proceedings of 34<sup>th</sup> International Conference on Software Engineering (**ICSE 2012**), Zurich, Switzerland, Jun 2012. Pages 80-90. Acceptance rate 21%.
- C53. **Vijay Ganesh**, Adam Kiezun, Shay Artzi, Philip Guo, Pieter Hooimiejer and Michael Ernst. HAMPI: A String Solver for Testing, Analysis and Vulnerability Detection. In Proceedings of 23<sup>rd</sup> International Conference on Computer-aided Verification (**CAV 2011**), Snowbird, USA, July 2011. Pages 1-19. [Invited Tutorial Paper at CAV 2011](#)
- C54. Karthick Jayaraman, **Vijay Ganesh**, Mahesh Tripunitara, Steve Chapin and Martin C. Rinard. Automatic Error Finding for Access-control Policies. In the Proceedings of the 13<sup>th</sup> ACM Conference on Computer and Communications Security (**CCS 2011**), Chicago, Illinois, USA, November 2011. Pages 163-174. Acceptance Rate 15%.
- C55. Adam Kiezun, **Vijay Ganesh**, Philip J. Guo, Pieter Hoomijier, and Michael D. Ernst. HAMPI: A Solver for String Constraints. In Proceedings of the 18<sup>th</sup> ACM International Symposium of Testing and Analysis (**ISSTA 2009**), Chicago, USA, July 2009. Pages 105-116. Acceptance Rate 29%. [ACM Distinguished \(SIGSOFT\) Paper Award at ISSTA 2009](#)
- C56. **Vijay Ganesh**, Tim Leek, and Martin C. Rinard. Taint-based Directed Whitebox Fuzzing. In the Proceedings of the 31<sup>st</sup> International Conference on Software Engineering (**ICSE 2009**), Vancouver, Canada, May 2009. Pages 474-484. Acceptance rate 12%.
- C57. Karthick Jayaraman, **Vijay Ganesh**, David Harvison, Vijay Ganesh and Adam Kiezun. jFuzz: A Concolic Whitebox Fuzzer for Java. In the Proceedings of NASA Formal Methods Symposium (**NFM 2009**), Mountain View, CA, USA, April 2009. Pages 121-125.
- C58. **Vijay Ganesh** and David L. Dill. A Decision Procedure for Bit-vectors and Arrays. In the Proceedings of the 19<sup>th</sup> International Conference on Computer Aided Verification (**CAV 2007**), Berlin, Germany, July 2007. Pages 519-531. Acceptance Rate 25%
- C59. Cristian Cadar, **Vijay Ganesh**, Peter Pawlowski, David L. Dill, and Dawson Engler. EXE: Automatically Generating Inputs of Death. In the Proceedings of the 13<sup>th</sup> ACM Conference on Computer and Communications Security (**CCS 2006**) Alexandria, Virginia, USA, November 2006. Pages 322-335. Acceptance Rate 15%. [ACM Test of Time Award at CCS 2016](#)
- C60. Sergey Berezin, **Vijay Ganesh**, and David Dill. An Online Proof-Producing Decision Procedure for Mixed-Integer Linear Arithmetic. In the Proceedings of the 9<sup>th</sup> International Conference on Tools & Algorithms for the Construction & Analysis of Systems (**TACAS 2003**), Warsaw, Poland, Apr 2003. Pages 521-536.

- C61. **Vijay Ganesh**, Sergey Berezin, and David L. Dill. Deciding Presburger Arithmetic by Model Checking and Comparisons with Other Methods. In the Proceedings of the 4<sup>th</sup> International Conference on Formal Methods for Computer Aided Design (**FMCAD 2002**), Portland, Oregon, USA, November 2002. Pages 171-186.
- C62. Ashok Halambi, Peter Grun, **Vijay Ganesh**, Asheesh Khare, Nikil Dutt, and Alex Nicolau. EXPRESSION: A Language for Architecture Exploration through Compiler/Simulator Retargetability. In the Proceedings of International Conference on Design Automation and Test in Europe (**DATE 1999**), Munich, Germany, March 1999. Pages 485-490.  
[Ten-year Most Influential Paper at DATE 2008](#)

#### PEER-REVIEWED JOURNAL PUBLICATIONS

- J1. Curtis Bright\*, Ilias Kotsireas, Albert Heinle, and **Vijay Ganesh**. Complex Golay Pairs up to Length 28: A Search via Computer Algebra and Programmatic SAT. Journal of Symbolic Computation (**JSC 2021**). Volume 102, January 2021. Pages 153-172.  
[In Special Issue of JSC 2021.](#)
- J2. Curtis Bright\*, Ilias Kotsireas, and **Vijay Ganesh**. Applying Computer Algebra Systems and SAT Solvers to the Williamson Conjecture. Journal of Symbolic Computation (**JSC 2020**). Volume 100, Dec 2020. Pages 187-209.  
[In Special Issue of JSC 2020](#)
- J3. Sebastian Wetzel, Roger Melko, Joseph Scott\*, Maysum Panju, and **Vijay Ganesh**. Discovering Symmetry Invariants and Conserved Quantities by Interpreting Siamese Neural Networks. Physical Review Research (**PRR 2020**), Volume 2, Issue 3, Sep 2020.
- J4. Curtis Bright\*, Kevin K. H. Cheung, Brett Stevens, Dominique Roy, Ilias Kotsireas, and **Vijay Ganesh**. A Non-existence Certificate for Projective Planes of Order Ten with Weight 15 Codewords. Springer Journal for Applicable Algebra for Engineering, Communications, and Computing (**AAECC 2020**). Volume 31, Issue 3-4, Mar-Apr 2020. Pages 195-213.
- J5. Curtis Bright\*, Ilias Kotsireas, and **Vijay Ganesh**. New Infinite Families of Perfect Quaternion and Williamson Sequences. IEEE Transactions on Information Theory (**IEEE Trans. Inf. Theory 2019**). Volume 66, Issue 12, Dec 2020. Pages 7739-7751.
- J6. Curtis Bright\*, Ilias Kotsireas, and **Vijay Ganesh**. The SAT+CAS Paradigm and the Williamson Conjecture (extended abstract). ACM Communications in Computer Algebra (**ACM CCA 2019**), Volume 52, Issue 3, September 2019. Pages 82-84.
- J7. Curtis Bright\*, Dragomir Djokovic, Ilias Kotsireas, and **Vijay Ganesh**. The SAT+CAS method for Combinatorial Search with Applications to Best Matrices. Annals of Mathematics and Artificial Intelligence (**AMAI 2019**). Volume 87, Dec 2019. Pages 321-342.
- J8. Jianmei Guo, Jia Hui Liang\*, Kai Shi, Dingyu Yang, Jingsong Zhang, **Vijay Ganesh**, Krzysztof Czarnecki, and Huiqun Yu. SMTIBEA: A Hybrid Multi-Objective Optimization Algorithm for Configuring Large Constrained Software Product Lines. International Journal of Software and System Modeling (**SOSM 2019**). Volume 18, Issue 2, August 2019. Pages 1447-1466.

- J9. Yunhui Zheng, **Vijay Ganesh**, Sanu Subramanian\*, Omer Tripp, Julian Dolby, and Xiangyu Zhang. Z3str2: An Efficient Solver for Strings, Regular Expressions, and Length Function. *Formal Methods in System Design Journal (FMSD 2017)*, Volume 50, Issue number 2-3, June 2017. Pages 249-288. [Invited Paper in the Formal Methods in System Design Journal 2017](#)
- J10. Ed Zulkoski\*, Curtis Bright\*, Albert Heinle, Ilias Kotsireas, Krzysztof Czarnecki, and **Vijay Ganesh**. Combining SAT Solvers with Computer Algebra Systems to Verify Combinatorial Conjectures. In the *Journal of Automated Reasoning (JAR 2017)*, Volume 58, Issue 3, March 2017. Pages 313-339. [Invited Paper in Special Issue of Journal of Automated Reasoning 2017](#)
- J11. Karthick Jayaraman, Mahesh Tripunitara, **Vijay Ganesh**, Steve Chapin, and Martin C. Rinard. Mohawk: Abstraction-refinement and Bound Estimation for Verifying Access-control Policies. In *ACM Transactions on Information and System Security (TISSEC 2013)*, Volume 15, Issue number 4, April 2013. Pages 18:1 – 18:28.
- J12. **Vijay Ganesh**, Adam Kiezun, Shay Artzi, Phillip Guo, Pieter Hooimiejer, and Michael D. Ernst. HAMPI: A Solver for Word Equations over Strings, Regular Expressions and Context-free Grammars. In *ACM Transactions on Software Engineering and Methodology (TOSEM 2012)*, Volume 21, Issue number 4, Nov 2012. Pages 25:1 – 25:28. [Invited Paper in TOSEM Journal 2012](#)
- J13. Cristian Cadar, **Vijay Ganesh**, Peter Pawlowski, David L. Dill, and Dawson Engler. EXE: Automatically Generating Inputs of Death. *ACM Transactions on Information and System Security (TISSEC 2008)*, Volume 12, Issue number 2, December 2008. Pages 10:1-10:38.

#### PEER-REVIEWED WORKSHOP PUBLICATIONS

- W1. Vineel Nagisetty, Laura Graves, and **Vijay Ganesh**. xAI-GAN: Enhancing Generative Adversarial Networks via Explainable AI Systems. Accepted at **AAAI-xAI 2021**.
- W2. Curtis Bright, Kevin K. H. Cheung, Brett Stevens, Ilias S. Kotsireas, and **Vijay Ganesh**. Non-existence Certificates for Ovals in a Projective Plane of Order Ten. In the Proceedings of the 31<sup>st</sup> International Workshop on Combinatorial Algorithms (**IWOCA 2020**). Virtual Conference (originally planned for Bordeaux, France), Jun 8 – Jun 10, 2020.
- W3. Gereon Kramer, Erika Abraham, and **Vijay Ganesh**. Proof Complexity of MCSAT Solvers. In the Proceedings of the 4<sup>th</sup> International Workshop on Satisfiability Checking and Symbolic Computation (**SC<sup>2</sup> 2019**), Bern, Switzerland, 10<sup>th</sup> July 2019.
- W4. Ed Zulkoski\*, Robert Robere, Jia Hui Liang\*, Ruben Martins, Christoph Wintersteiger, Krzysztof Czarnecki, and **Vijay Ganesh**. Relating Complexity-theoretic Parameters with SAT Solver Performance. In *Pragmatics of Constraint Reasoning Workshop (PoCR 2017)*, Melbourne, Australia, Aug 28-Sep 1, 2017.
- W5. **Vijay Ganesh**, Sebastian Benascu, and Martin Ochoa. The Meaning of Attack-resistant Systems. In Proceedings of International Workshop on Programming Languages and Analysis for Security (**PLAS @ ECOOP 2015**), Prague, Czech Republic, July 6, 2015. Pages 49-55.



- W6. Nikolaj Bjorner, **Vijay Ganesh**, Raphael Michel, and Margus Veanes. An SMT-LIB Format for Sequences and Regular Expressions. In the Proceedings of the International Workshop on Satisfiability Modulo Theories (**SMT 2012**), Manchester, UK, June 30, 2012. Pages 77-87.
- W7. Raphael Michel, **Vijay Ganesh**, Arnaud Hubaux, and Patrick Heymans. An SMT-based Approach to Automated Configuration. In the Proceedings of the International Workshop on Satisfiability Modulo Theories (**SMT 2012**), Manchester, UK, June 30, 2012. Pages 109-119.
- W8. **Vijay Ganesh**, Michael Carbin and Martin C. Rinard. Cryptographic Path Hardening: Hiding Vulnerabilities in Software using Cryptography. Off-the-beaten-track. Co-located with Principles of Programming Languages Conference, Philadelphia, USA, Jan 2012.
- W9. Saddek Bensalem, **Vijay Ganesh**, et al. An Overview of SAL. In Proceedings of NASA Langley Formal Methods Workshop (**LFM 2000**), Williamsburg, Virginia, USA, June 2000.

#### EDITED VOLUMES

- E1. Cristian Cadar, **Vijay Ganesh**, Raimondas Sasnauskas, and Koushik Sen. Symbolic Execution and Constraint Solving. Dagstuhl Seminar 14442, Volume 4, Issue 10, **Dagstuhl Reports 2015**.
- E2. Armin Biere, **Vijay Ganesh**, Martin Grohe, Jakob Nordström, and Ryan Williams. The Theory and Practice of SAT Solving. Dagstuhl Seminar 15171, Volume 5, Issue 4, **Dagstuhl Reports 2015**.
- E3. **Vijay Ganesh** and Nicky Williams. Constraints in Software Testing, Verification, and Analysis (**CSTVA 2014**), ACM 2014. ISBN 978-1-4503-2847-0.

#### INVITED TALKS

---

Institution/Venue (significant venues or talks highlighted below in boldface)	Date	Talk Title
1. Waterloo Computational Mathematics Colloquium, University of Waterloo, Ontario, Canada	Oct 2020	Machine Learning and Logic Solvers: The Next Frontier
<b>2. International Congress on Mathematical Software, Braunschweig, Germany</b>	<b>Jul 2020</b>	<b>Machine Learning and Logic Solvers: The Next Frontier</b>
3. Vector Institute, Toronto, Canada	Feb 2020	Machine learning and Logic Solvers: The Next Frontier
4. Indian Institute of Technology, Bombay, India	Dec 2019	Machine Learning and Logic Solvers: The Next Frontier
5. Sorbonne University, Paris, France	Sep 2019	Machine Learning for SAT Solvers
6. Hasso Plattner Institute, Potsdam, Germany	Aug 2019	Machine Learning for SAT Solvers



<b>7. Keynote at International Symposium on Software Testing and Analysis (ISSTA), Beijing, China</b>	<b>July 2019</b>	<b>ACM IMPACT Paper Award: Theory and Practice of String Solvers</b>
8. Indian SAT/SMT School, IIIT, Hyderabad, India	Dec 2018	SAT and SMT Solvers: A Foundational Perspective (3 lectures)
9. Waterloo AI Institute, Canada	Oct 2018	Machine Learning for SAT Solvers
10. Marktoberdorf Summer School on Dependable and Secure Software Systems, Marktoberdorf, Germany	Sep 2018	SAT and SMT Solvers: A Foundational Perspective (4 lectures)
<b>11. Theory and Practice of Satisfiability Solving, BIRS, Oaxaca, Mexico</b>	<b>Aug 2018</b>	<b>Machine Learning for SAT Solvers</b>
<b>12. The 24<sup>th</sup> Conference on Applications of Computer Algebra (ACA 2018), Santiago De Compostela, Spain</b>	<b>Jun 2018</b>	<b>Plenary Talk: SAT Solvers and Computer Algebra Systems: A Powerful Combination for Mathematics</b>
13. University of Kiel, Germany	Apr 2018	Mergeability and the Unreasonable Effectiveness of SAT Solvers
14. East China University of Science & Technology, Shanghai, China	Apr 2018	On the Unreasonable Effectiveness of SAT Solvers
15. Academia Sinica, Taipei, Taiwan	Apr 2018	On the Unreasonable Effectiveness of SAT Solvers
16. National University of Singapore	Apr 2018	On the Unreasonable Effectiveness of SAT Solvers
17. Microsoft Research, Bangalore, India	Jan 2018	On the Unreasonable Effectiveness of SAT Solvers
18. Indian Institute of Science, Bangalore, India	Dec 2018	On the Unreasonable Effectiveness of SAT Solvers
19. CSTVA 2017 Workshop, Melbourne, Australia	Aug 2017	On the Unreasonable Effectiveness of SAT Solvers
20. David Dill @ 60 Workshop, Heidelberg, Germany	Jul 2017	On the Unreasonable Effectiveness of SAT Solvers
21. University of Luxembourg	Jul 2017	On the Unreasonable Effectiveness of SAT Solvers
22. Hasso Plattner Institute, Potsdam, Germany	Jul 2017	On the Unreasonable Effectiveness of SAT Solvers
23. Rice University, Houston, USA	Jun 2017	On the Unreasonable Effectiveness of SAT Solvers
24. University of Wisconsin, Madison, USA	Jun 2017	On the Unreasonable Effectiveness of SAT Solvers

25. University of Washington, Seattle, USA	Jun 2017	On the Unreasonable Effectiveness of SAT Solvers
26. Microsoft Research, Redmond, USA	Jun 2017	On the Unreasonable Effectiveness of SAT Solvers
27. Achim Kempf Research Group, Waterloo, Canada	Jun 2017	On the Unreasonable Effectiveness of SAT Solvers
28. IQC, Waterloo, Canada	Jun 2017	On the Unreasonable Effectiveness of SAT Solvers
29. Inria/Loria, Nancy, France	Apr 2017	On the Unreasonable Effectiveness of SAT Solvers
30. Max Planck Institute, Saarbrucken, Germany	Apr 2017	On the Unreasonable Effectiveness of SAT Solvers
31. Moscow State University, Moscow, Russia	Apr 2017	On the Unreasonable Effectiveness of SAT Solvers
32. College of Engineering, Trivandrum, India	Sep 2016	Towards a Deeper Empirical Understanding of CDCL SAT Solvers
<b>33. Institute for Mathematical Sciences, NUS, Singapore</b>	<b>Sep 2016</b>	<b>Towards a Deeper Understanding of Branching Heuristics in SAT Solvers</b>
34. Fields Institute, Toronto, Canada	Aug 2016	Towards a Deeper Understanding of Branching Heuristics in SAT Solvers
<b>35. Keynote at CSTVA, Saarbrucken, Germany</b>	<b>Jul 2016</b>	<b>Towards a Deeper Empirical Understanding of CDCL SAT Solvers</b>
36. Moscow State University, Moscow, Russia	Apr 2016	Towards a Deeper Empirical Understanding of CDCL SAT Solvers
37. St. Petersburg State, Chebyshev Labs, Russia	Apr 2016	Towards a Deeper Empirical Understanding of CDCL SAT Solvers
38. SRI International, Menlo Park, CA, USA	Jul 2015	Towards a Deeper Empirical Understanding of CDCL SAT Solvers
39. University of California, Berkeley, CA, USA	Jul 2015	Towards a Deeper Empirical Understanding of CDCL SAT Solvers
40. Moscow State University, Russia	Jun 2015	Towards a Deeper Empirical Understanding of CDCL SAT Solvers
41. Dagstuhl, Saarland, Germany	Apr 2015	Towards a Deeper Empirical Understanding of CDCL SAT Solvers
42. Computer Algebra Group, U. of Waterloo, Canada	Mar 2015	An Introduction to SAT/SMT Solvers
43. Dagstuhl, Saarland, Germany	Feb 2015	Impact of Community Structure on SAT Solver Performance
44. Institute of Mathematical Sciences, Chennai, India	Feb 2015	Impact of Community Structure on SAT Solver Performance

45. MapleSoft Inc., Waterloo, Canada	Dec 2014	Solvers for Software Reliability and Security
46. IBM PL Day, TJ Watson Center, NY, USA	Nov 2014	Impact of Community Structure on SAT Solver Performance
47. Dagstuhl, Saarland, Germany	Oct 2014	SAT/SMT Solvers and Applications: Key Ideas and Future Directions
48. Dagstuhl, Saarland, Germany	Aug 2014	Impact of Community Structure on SAT Solver Performance
49. <b>Banff Mathematical Research Station, Canada</b>	<b>Jan 2014</b>	<b>VSIDS Branching Heuristic and Timed Graph Centrality</b>
50. Institute of Mathematical Sciences, Chennai, India	Dec 2013	Undecidability Results for Word Equations, Regular Expressions, and Length Function
51. Aspiring Minds, New Delhi, India	Dec 2013	Solvers for Software Reliability and Security
52. ICCC 2013, College of Engineering, Trivandrum, India	Dec 2013	Solvers for Software Reliability and Security
53. ADDCT 2013, Lake Placid, NY, USA	Jun 2013	Undecidability Results for Word Equations, Regular Expressions, and Length Function
54. Google Inc., NY, USA	Jun 2013	Solvers for Software Reliability and Security
55. HCSS, Annapolis, MD, USA	May 2013	String Solvers for Reliability and Security
56. Kesterel Institute, Palo Alto, CA, USA	May 2013	Solvers for Software Reliability and Security
57. Purdue University, IN, USA	May 2013	Solvers for Software Reliability and Security
58. University of Iowa, Iowa City, USA	May 2013	Solvers for Software Reliability and Security
59. Dagstuhl, Saarland, Germany	Feb 2013	SAT/SMT Solvers for Reliability, Security, and Repair
60. <b>Keynote at CSTVA'12, Montreal, Canada</b>	<b>Apr 2012</b>	<b>Solvers for Software Reliability and Security</b>
61. Dagstuhl, Saarland, Germany	Feb 2012	SAT/SMT Solvers for Reliability and Security
62. <b>CAV 2011 Invited Tutorial Snowbird, Utah, USA</b>	<b>Jul 2011</b>	<b>HAMPI: A String Solver for Testing, Analysis &amp; Vulnerability Detection</b>
63. Dagstuhl, Saarland, Germany	Aug 2011	SAT/SMT Solvers for Software Reliability and Security
64. Dagstuhl, Saarland, Germany	Jul 2011	SAT/SMT Solvers for Software Reliability and Security

65. Dagstuhl, Saarland, Germany	Apr 2010	SAT/SMT Solvers for Software Reliability and Security
66. Massachusetts Institute of Technology Lincoln Labs, USA	Feb 2008	Constraint Solvers for Program Analysis and Bug-finding
67. Massachusetts Institute of Technology, Cambridge, USA	Nov 2007	Constraint Solvers for Program Analysis and Bug-finding
68. Coverity Inc. San Francisco, USA	Sep 2007	The STP Bit-vector and Array Solver

## TEACHING

---

### COURSES DEVELOPED

**Computer-aided Reasoning for Software Engineering (ECE 750-T28):** At the University of Waterloo, I developed a graduate course on computer-aided reasoning (SAT/SMT solvers and proof assistants) and their applications in software engineering and security. The course is divided into three modules: In the first module, I cover the basics of mathematical logic. In the second module, I cover modern conflict-driven clause-learning SAT solvers, SMT solvers, their design and architecture, combination of theories, DPLL(T) etc. Finally, in the third module I cover application of SAT/SMT solvers to verification of software systems, with a special focus on symbolic execution-based testing and analysis. The course had a project component, and the students were required to build a system based on SAT or SMT solvers as part of their project.

**Discrete Mathematics and Logic (ECE 208):** At the University of Waterloo, I developed a theory undergraduate course (ECE 208) for ECE students who may not have had any background in logic, computability and complexity theory. The course is quite comprehensive, i.e., covers Boolean logic, first-order logic, automata and formal language theory, and some basics of complexity theory. It also has a practical component where the students have to apply the concepts learnt in class in a practical setting (e.g., develop a DPLL SAT solver).

### COURSES TAUGHT

Term and Year	Course Number/Name	Enrollment
Fall 2020 (Undergraduate)	ECE208 (Discrete Mathematics and Logic)	191
Spring 2020 (Graduate)	ECE653 (Software Testing, Quality Assurance, and Maintenance)	92
Spring 2019 (Undergraduate)	ECE208 (Discrete Mathematics and Logic)	140
Fall 2018 (Graduate)	ECE 750-T28 (Computer-aided Reasoning)	4
Spring 2018 (Undergraduate)	ECE 351 (Introduction to Compilers)	160
Fall 2017 (Graduate)	ECE 750-T28 (Computer-aided Reasoning)	5

Spring 2017 (Undergraduate)	ECE 458 (Introduction to Computer Security)	134
Spring 2017 (Undergraduate)	ECE 351 (Introduction to Compilers)	132
Fall 2016 (Graduate)	ECE 750-T28 (Computer-aided Reasoning)	12
Fall 2015 (Undergraduate)	ECE 250 (Algorithms and Data Structures)	129
Winter 2015 (Graduate)	ECE 750-T28 (Computer-aided Reasoning)	7
Winter 2015 (Undergraduate)	ECE 351 (Introduction to Compilers)	69
Spring 2014 (Undergraduate)	ECE 458 (Introduction to Computer Security)	76
Spring 2014 (Undergraduate)	ECE 351 (Introduction to Compilers)	58
Winter 2014 (Undergraduate)	ECE 351 (Introduction to Compilers)	84
Fall 2013 (Graduate)	ECE 750-T28 (Computer-aided Reasoning)	15
Winter 2013 (Undergraduate)	ECE 458 (Introduction to Computer Security)	74

## SUPERVISION

---

From 2011-present, I have co-advised 2 postdoctoral fellows (one was previously my PhD student) and 7 PhD students. Of these, currently 2 are tenure-track or tenured professors, 1 is a lecturer, 4 others are researchers at companies such as IBM, Amazon, Microsoft and Quantstamp, and 1 is a software engineer at Google. I have also co-advised or mentored 11 master's, and further mentored around two dozen bachelor's students. All of them are now gainfully employed at top tech companies or pursuing graduate studies.

## CURRENT STUDENTS AND POSTDOCTORAL FELLOWS (PDFs)

Degree	Name	Advisor	Start	Research topic	End
PhD	Murphy Berzish	Vijay Ganesh	09/2016	Algorithms for string solving	2021
PhD	Joe Scott	Vijay Ganesh	09/2017	Deep learning and SAT solving	2021
PhD	Ian Li	Vijay Ganesh	09/2019	Restarts in SAT solvers	2023
MASc	Alaina Mahalanobis	Vijay Ganesh	09/2020	xAI-based GANs	2022

MASc	Abinaya Venkatesan	Vijay Ganesh	09/2020	SAT Solvers for Exact Circuit Complexity	2022
MASc	Laura Graves	Vijay Ganesh	09/2019	Testing and Verification of ML	2021
MASc	Vineel Nagisetty	Vijay Ganesh	09/2019	xAI-based GANs	2021
MASc	Behkish Nassirzadeh	Vijay Ganesh	05/2019	SAT-based Cryptanalysis	2021

### GRADUATED STUDENTS AND POSTDOCTORAL FELLOWS (PDFs)

Degree	Name	Lead Supervisor	Co-supervisor	Grad date	Research Topic	Current Status
PDF, Waterloo	Curtis Bright	Vijay Ganesh		2019	SAT+CAS Combination for Mathematics	Assistant Professor, University of Windsor, Canada
PDF, Waterloo	Souraditya Paul	Vijay Ganesh		2014	Cryptanalysis of hash functions	Associate Professor, IIT, Bhilai, India
PhD, Waterloo	Saeed Nejati	Vijay Ganesh	Cathy Gebotys	2020	SAT-based Cryptanalysis	Applied Scientist, Amazon, Seattle, USA
PhD, Waterloo	Reza Babaee	Vijay Ganesh	Derek Rayside	2019	Machine Learning based Runtime Verification	Lecturer, University of Waterloo
PhD, Waterloo	Jia Hui (Jimmy) Liang	Vijay Ganesh	Krzysztof Czarnecki	2018	Machine Learning for SAT solvers	Senior software engineer at Google
PhD, Waterloo	Ed Zulkoski	Vijay Ganesh	Krzysztof Czarnecki	2018	Complexity-theoretic parameters of SAT formulas	Senior software engineer at Quantstamp
PhD, Waterloo	Curtis Bright	Vijay Ganesh	Krzysztof Czarnecki	2017	SAT+CAS Combination for Mathematics	Postdoctoral Fellow, Waterloo
PhD, Purdue	Yunhui Zheng*	Xiangyu Zhang Purdue U.	Vijay Ganesh	2014	String solvers for web security analysis	Researcher, IBM TJ Watson Center, NY
PhD, Syracuse	Karthick Jayaraman*	Steve Chapin Syracuse U.	Vijay Ganesh	2010	Security analysis of web applications	Software Engineer, Microsoft, Redmond, USA
MASc	Hari Govind	Arie Gurfinkel	Vijay Ganesh	2017	Interpolating Strong Induction	2019
MASc	Ian Li	Vijay Ganesh		2017	Complexity of restarts in SAT solvers	2019



MASc, Waterloo	Dmitry Blotsky	Vijay Ganesh		2018	Fuzzers for string solvers	Software Engineer at Amazon
MEng, Waterloo	Mark Wheatley	Vijay Ganesh		2018	Symbolic execution-based testing	Software Engineer at BlackBerry
MASc, Waterloo	Riyad Parvez	Vijay Ganesh	Paul Ward	2016	Combining static and symbolic analysis	
MASc, Waterloo	Sanu Subramanian	Vijay Ganesh		2015	String and bit-vector solvers for security	Security Engineer, Intel, Waterloo
MASc, Waterloo	Zack Newsham	Vijay Ganesh	Sebastian Fischmeister	2015	Community structure of Boolean SAT instances	Tech lead, Mushroom Cloud, Toronto
MS, EPFL	Philippe Suter	Viktor Kuncak EPFL	Vijay Ganesh	2008	Combination of decision procedures	Researcher, IBM TJ Watson Center, NY

\*I was an unofficial PhD advisor to Yunhui Zheng and Karthick Jayaraman.

## SERVICE AND PROFESSIONAL ACTIVITIES

### EDITORIAL POSITIONS AND STEERING COMMITTEE MEMBER

- **Editor-in-Chief**
  - Springer Birkhauser Book Series titled “Progress in Computer Science and Applied Logic” (**PCSAL**). Jan 2018-present
- **Member of Editorial Board**
  - Journal of Satisfiability (**JSAT**). Oct 2018-present
- **Steering Committee Member**
  - Satisfiability Checking and Symbolic Computation (SC<sup>2</sup>) Workshop. 2017-present
  - SAT/SMT/AR Summer School. 2018-present
  - CSTVA Workshop. 2017-present

### TECHNICAL PROGRAM COMMITTEES, CHAIR AND REFEREE POSITIONS

Year	Position	Venue
2021	Co-Organizer	1) Simons Institute Semester on “Satisfiability: Theory, Practice, and Beyond”, Simons Institute @ Berkeley, USA 2) Waterloo ML + Logic Online Colloquium 3) Dagstuhl Seminar on ML + Logic 4) Theory and Practice of String Solving (TPSS Workshop @ CAV 2021)
2021	PC Co-chair	ATVA 2021
2021	Senior PC Member	IJCAI 2021 (Senior PC Member)
2021	PC Member	CAV 2021, PLDI 2021, AAI 2021, FM 2021, SOCS 2021, AAI-xAI 2021
2020	PC Member	POPL 2020, AAI 2020, IJCAI 2020, ICTAI 2020

2020	Co-organizer	Dagstuhl seminar: Theory and Practice of SAT Solving (postponed to 2021 due to the COVID pandemic)
2019	PC Member	IJCAI 2019, ICISS 2019, ICTAI 2019
2019	Co-organizer	1) Dagstuhl Seminar: Bringing CP, SAT, and SMT together: Next Challenges in Constraint Solving 2) Waterloo Machine Learning and Security Workshop 3) Waterloo Blockchain and Security Workshop
2018	PC Member	CAV 2018, IJCAI 2018, CP 2018, FM 2018, FCSD 2018, IJCAR 2018, SAT 2018, PoS 2018
2017	PC Member	PLDI 2017 (ERC), ICSE 2017 (NIER), CP 2017, FroCoS 2017, ASL Special Session on Computer-aided Proofs 2017, SYNASC 2017, SC <sup>2</sup> 2017
2017	Co-chair	1) Association of Symbolic Logic Special Session on Computer-aided Proofs 2017 2) Satisfiability Checking and Symbolic Computation (SC <sup>2</sup> ) Workshop 2017 3) David Dill @ 60 Workshop held at CAV 2017
2016	PC Member	POPL 2016 (ERC), ISAIM 2016, ICDCIT 2016, ICCS 2016, FM 2016, PAAR 2016, VSTTE 2016, SC <sup>2</sup> 2016, USE 2016
2016	Main Organizer	Fields Institute Workshop on Theoretical Foundations of SAT Solving, Toronto, Canada. Aug 15-19, 2016
2015	PC Member	AAAI 2015, FM 2015, SMT 2015, VSTTE 2015, USE 2015, ASSESS 2015, CCS-SPSM 2015
2015	Co-chair and Steering Committee	SMT 2015 SMT Workshop 2015
2015	Co-organizer	Dagstuhl seminar: Theory and Practice of SAT Solving, Apr 19-24, 2015
2014	PC Member	ASSESS 2014, CSTVA 2014
2014	Co-chair	Constraint Solvers for Testing, Verification, and Analysis 2014. Held alongside ICSE 2014
2014	Co-organizer	Dagstuhl seminar: Symbolic Execution and Solving, Oct 27-30, 2014
2013	PC Member	FroCos 2013, CSTVA 2013
2012	PC Member	SMT 2012, IEEE NCA 2012
2011	PC Member	SMT 2011, IEEE NCA 2011
2011	Organizer	International Summer School on SAT/SMT Solvers at MIT, Cambridge, MA, USA. June 12-17, 2011
2004	Organizer	International School on Combination of Decision Procedures, SRI International and Stanford, Aug 6-12, 2004

## JOURNAL REVIEWER

- Mathematical Reviews (MR) – American Mathematical Society
- Journal of Artificial Intelligence Research (JAIR) – AAAI Press
- Journal of Automated Reasoning (JAR) – Springer
- Artificial Intelligence Journal (AI) – Elsevier
- Formal Methods in Systems Design (FMSD) – Springer
- Communication of the ACM (CACM) – ACM
- Algorithms and Complexity in Mathematics, Epistemology, and Science (ACMES)
- ACM Transactions on Software Engineering and Methodology (TOSEM)
- ACM Transactions on Software System and Information Security (TISSEC)
- ACM Transactions on Design Automation of Electronic Systems (TOADES)
- IEEE Transactions on Dependable and Securing Computing (TDSC)
- IEEE Transactions on Software Engineering (TSE)
- IEEE Computer Journal
- IEEE Transactions on Reliability
- European Journal of Combinatorics
- Acta Informatica
- AI Communications
- Software Testing, Verification, and Reliability (STVR) – Wiley

## INTERNATIONAL REFEREE POSITIONS

- National Science Foundation (NSF), USA, External Reviewer
- Royal Swedish Academy of Sciences, External Reviewer
- European Research Council (ERC), External Reviewer
- Icelandic Science Council (IRC), External Reviewer
- Natural Sciences and Engineering Research Council (NSERC), Canada, Reviewer

## UNIVERSITY AND DEPARTMENTAL COMMITTEES

- University of Waterloo, ECE Department Faculty Hiring Committee Member, 2017 - present
- University of Waterloo, ECE Department Research Committee, 2017
- University of Waterloo, Engineering Faculty Council, 2013-2014, 2020-present
- University of Waterloo, ECE Department CGS and Vanier Scholarship Committee, 2014
- University of Waterloo, SE/ECE Capstone Design Symposium Referee, 2014 and 2015

## PhD/MS DEFENSE COMMITTEE MEMBER\*

Name	Degree	University	Supervisor	Year
Thibaud Lutillier	PhD	Waterloo	Lin Tan	2020
Mahsa Emam Tabi	PhD	Waterloo	Ladan Tahvildari	2018

Frank Imeson	PhD	Waterloo	Stephen Smith	2017
Vajih Montaghani	PhD	Waterloo	Derek Rayside	2017
Albert Heinle	PhD	Waterloo	Mark Giesbrecht	2016
Ana Sima Claudia	MS	EPFL	George Candea	2015
Elaheh Fata	MASc	Waterloo	Shreyas Sundaram	2013

\* students not under my co-supervision

#### PhD/MS COMPREHENSIVE EXAM COMMITTEE MEMBER/THESIS READER\*

Name	Role	Supervisor	Year
Hari Govind	PhD Comp Exam Committee	Arie Gurfinkel	2020
Thibaud Lutillier	PhD Comp Exam Committee	Lin Tan	2017
Steven Stewart	MS Comp Exam Committee	Derek Rayside	2015
Frank Imeson	PhD Comp Exam Committee	Steven Smith	2015
Mahsa Emam Tabi	PhD Comp Exam Committee	Ladan Tahvildari	2014
Quinn Hamm	MASc Thesis Reader	Lin Tan	2014
Lie Zhang	MASc Thesis Reader	Lin Tan	2014
Vajih Montaghani	PhD Comp Exam Committee	Derek Rayside	2013
Keyvan Golestan	PhD Comp Exam Committee	Fakhri Karray	2013

\* students not under my co-supervision

#### SOFTWARE DEVELOPED

---

The primary focus of my research is the theory and practice of mathematical reasoning or constraint solving algorithms (aka SAT and SMT solvers), and in this context, I have led the development of the following solvers and mathematical reasoning: the STP bit-vector and array solver, the HAMPI string solver, the Z3 family of string solvers (Z3str3 and its predecessors Z3str2 and Z3str), the MapleSAT family of Boolean SAT solvers (MapleCOMSPS, MapleSAT etc.), the MaplePainLeSS parallel SAT solver-based cryptanalysis tools, and the MathCheck conjecture verifier. In addition to constraint solvers, I have also led the development of around dozen software tools such as automatic software testers, compilers, symbolic simulation engines, instruction-set simulators, retargetable compilers for hardware languages, and math conjecture verifiers. Many of my tools are currently in use in more than 100 significant projects in academia and industry.

**The MapleSAT Boolean SAT solver** is a tool that combines machine-learning based branching and restart heuristics with deduction, a la, conflict analysis. A variant of this solver won two gold medals at the

highly competitive SAT competition (main and application tracks) in 2016 and two silver medals at the SAT competition (main and no-limits track) in 2017.

**The STP Bitvector and Array Solver** is the backend for the KLEE, S2E, BAP, BitBlaze, WebBlaze, and Souper tools. It is used in dozens of companies including at Google, HP, and Apple. The STP solver won the highly competitive annual solver competition, SMTCOMP, in 2006/2010 and placed second in 2011/2014 (bit-vector category). The STP solver played an important role in the development of symbolic execution-based analysis and testing, widely considered a breakthrough in software engineering.

**The Z3str family of SMT solvers** support a rich theory of strings, regular expressions, and integers aimed at bug-finding, verification, and analysis of string-intensive programs. Additionally, we have also implemented a combination of decision procedure for theories over string equations and bit-vectors in Z3str3 that natively supports functions such as strcmp, strncmp, etc. aimed at analysis and testing of C/C++ programs. As of May 2017, Z3str3 string solver is now officially part of Microsoft's Z3 solver.

**MathCheck** is a tool that combines a SAT solver and a computer algebra system (CAS) aimed at finite verification or counter-example construction for combinatorial math conjectures. As of 2019, we have finitely verified several math conjectures up to bounds not previously attained or have constructed counterexamples for them. For example, using MathCheck we showed that the smallest counterexample to the Williamson conjecture is of order 35, thus settling a problem that had been open since 1944.

## SOFTWARE TOOLS

Name of Software	Purpose	Dates	Awards, Conference Venues, and Journals
<a href="#">MapleSAT family of SAT solvers</a>	A SAT solver using a reinforcement learning based branching heuristic	2015 – present	Winner of two silver medals at SAT 2017, and two gold medals at SAT competition 2016. SAT 2017/2016, AAI 2016, HVC 2015, SAT 2014
<a href="#">STP bit-vector and array solver</a>	A constraint solver for bit-vector and arrays	2005 – present	Winner of SMTCOMP (bit-vector) in 2006/2010, & second in 2011/2014. CAV 2007
<a href="#">Z3 family of String solvers</a>	A solver for string equations, regular expressions, and length	2013 – present	ICSE 2017, FMSD 2017 SMT 2016, CAV 2015, FSE 2013
<a href="#">MathCheck conjecture verifier</a>	A math conjecture verifier via a combination of SAT and CAS	2014 – present	JAR 2017, CASC 2016, Invited paper at IJCAI 2016, CADE 2015
<a href="#">Parallel SAT-based Cryptanalysis</a>	A parallel SAT solver using a ML based splitter	2016 – present	SAT 2017, CP 2018
MPro	Smart contract security analysis tool combining static & symbolic analysis	2019 – present	ISSRE 2019
Lynx	A programmatic Boolean SAT solver	2011 – 2012	SAT 2012

<a href="#">HAMPI</a>	A solver for string equations, and regular expressions	2009 – 2012	CAV 2011, ACM SIGSOFT Award at ISSTA 2009 (also, an invited paper at TOSEM 2012)
Mohawk	A model-checking tool for access-control policies	2010 – 2011	CCS 2011, TISSEC 2013
BuzzFuzz	A taint-based whitebox fuzzer for C programs	2008 – 2009	ICSE 2009
jFuzz	A concolic testing tool for Java	2009	NFM 2009

## REFERENCES

---

### **Professor Moshe Vardi**

Department of Computer Science  
 Mail Stop 132  
 Rice University, 6100 S. Main Street  
 Houston, TX, USA 77005-1892  
 Phone: +1-713-348-5977  
 Email: [vardi@cs.rice.edu](mailto:vardi@cs.rice.edu)

### **Professor Somesh Jha**

Computer Sciences Department  
 University of Wisconsin, Madison  
 1210 W. Dayton Street  
 Madison, WI, USA 53706  
 Phone: +1-608-262-9519  
 Email: [jha@cs.wisc.edu](mailto:jha@cs.wisc.edu)

### **Professor Ras Bodik**

Paul G. Allen School of Computer Science  
 and Engineering  
 University of Washington, Seattle  
 Bill and Melinda Gates Center, Room 243  
 3000 E Stevens Way NE  
 Seattle, WA, USA 98195  
 Phone: +1-206-616-7172  
 Email: [bodik@cs.washington.edu](mailto:bodik@cs.washington.edu)

### **Professor Martin Rinard**

Department of Computer Science  
 Massachusetts Institute of Technology, 32-G828  
 32 Vassar Street  
 Cambridge, MA, USA 02139  
 Phone: +1-617-258-6922  
 Email: [rinard@csail.mit.edu](mailto:rinard@csail.mit.edu)

### **Professor Sam Buss**

Department of Mathematics  
 University of California, San Diego  
 Office APM 7456  
 La Jolla, CA, USA 92093-0112  
 Phone: +1-858-534-6455  
 Email: [sbuss@ucsd.edu](mailto:sbuss@ucsd.edu)