Rohit Chadha

University of Missouri, Columbia, MO
Email: chadha.rohit@gmail.com, Phone: +1-573-424-5122
http://engineers.missouri.edu/chadhar/

Research Interests

Security, Formal Methods, Model Checking, Logic in Computer Science, Software Engineering

Education

Ph.D. **Department of Mathematics, University of Pennsylvania**, 2003, USA
Dissertation: A formal analysis of exchange of digital signatures
Advisor: Andre Scedrov

B.Tech. **Computer Sc. and Engg., Indian Institute of Technology, N. Delhi**, 1997, India

Employment

Associate Professor, September 2018-Present
Department of Computer Science, University of Missouri, Columbia

Assistant Professor, September 2012-2018
Department of Computer Science,University of Missouri, Columbia

INRIA Research Scientist, October 2009-August 2012
Laboratoire Spécification et Vérification, CNRS & ENS de Cachan, France

Visiting Fellow (Courtesy Appointment), March 2011-April 2011
Faculty of Engineering and Information Technology
Univ. of Technology, Sydney, Australia

Postdoctoral Research Associate, October 2006-August 2009
Dept. of Computer Science, Univ. of Illinois at Urbana-Champaign, Urbana, USA

Postdoctoral Research Fellow, September 2005-September 2006
Center for Logic and Computation, Dept. of Mathematics, IST, Lisboa, Portugal

Research Fellow August 2003-April 2005
Dept. of Informatics, Univ. of Sussex, UK

Software Engineer, July 1997-May 1998
Delsoft India Ltd, Noida, India

Awards and Distinctions

ACM/ThinkLoud Computing Reviews 21st Annual Best of Computing
Publication "Automated verification of equivalence properties of cryptographic protocols" recognized as one of the Notable Books and Articles of 2016

NSF Career Award, 2016

Grants

Research grants

Principal Investigator
CAREER: Automated analysis of security hyperproperties
National Science Foundation
Total Award: $436,035
Total Award Period Covered: 06-01-2016 to 05-31-2021

Principal Investigator
TWC: Medium: Collaborative: Automated formal analysis of security protocols with private coin tosses
National Science Foundation
Award: $244,810 MU portion (lead institution); shared credit: 100%, $800,000 total
Award Period Covered: 09-01-13 to 08-31-18

Workshop organization grants

Conference support for Midwest Verification Day, 2014
National Science Foundation
Award: $10,000
Award Period Covered: 08-06-14 to 01-13-15

Pending grant applications

SHF: CORE: Medium: Collaborative: Verification of Differential Privacy Mechanisms
National Science Foundation
Period Requested: July 16, 2018 to July 15, 2022

Publications

Book chapters

[1] Rohit Chadha, Paulo Mateus, Amilcar Sernadas, and Cristina Sernadas. Extending classical logic for reasoning about quantum systems. In D. Gabbay K. Engesser and D. Lehmann, editors, *Handbook of Quantum Logic and Quantum Structures: Quantum Logic*, pages 325–372. Elsevier, 2009.

Peer-reviewed journal articles

[1] Yue Ben, Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan. Decidable and Expressive Classes of Probabilistic Automata. *Journal of Computer and System Sciences.* Accepted.

[2] Rohit Chadha, Vincent Cheval, Ştefan Ciobaca and Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. *ACM Transactions on Computational Logic.* 17(4) 23:1–23:32, 2016. 32 pages + 50 page electronic index. Selected by ACM/ThinkLoud Computing Reviews as part of the 21st Annual Best of Computing list of Notable Books and Articles of 2016.

[3] Rohit Chadha, Mahesh Viswanathan and Ramesh Viswanathan. Least upper bounds for probability measures and their applications to abstractions. *Information and Computation.* 234:68-106, 2014. 39 pages.

[4] Rémi Bonnet, Rohit Chadha, P. Madhusudan and Mahesh Viswanathan. Reachability under Contextual Locking. *Logical Methods in Computer Science. (Special issue on Best Theoretical Papers of TACAS 2012).* 9(3), 2013. 17 pages.

[5] Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. Power of randomization in automata on infinite strings. *Logical Methods in Computer Science.* 7(3): 2011. 32 pages.

[6] Rohit Chadha and Mahesh Viswanathan. A counterexample guided abstraction-refinement framework for Markov Decision Processes. *ACM Transactions on Computational Logic*, 12(1):1–49, 2010. 49 pages.

[7] Rohit Chadha and Mahesh Viswanathan. Deciding branching-time properties for asynchronous programs. *Theoretical Computer Science*, 410(42):4169–4179, 2009. 11 pages.

[8] Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. On the expressiveness and complexity of randomization in finite state monitors. *Journal of the ACM*, 56(5): 26:1-26:44, 2009. 44 pages.

[9] Pedro Baltazar, Rohit Chadha, and Paulo Mateus. Quantum computation tree logic – model checking and complete calculus. *International Journal of Quantum Information*, 6(2):281–302, 2008. 22 pages.

[10] Rohit Chadha, Luis Cruz-Filipe, Paulo Mateus, and Amilcar Sernadas. Reasoning about probabilistic sequential programs. *Theoretical Computer Science*, 379(1-2):142–165, 2007. 26 pages.

[11] Rohit Chadha, Paulo Mateus, and Amilcar Sernadas. Reasoning about imperative quantum programs. *Electronic Notes in Theoretical Computer Science*, 158:19–39, 2006. 21 pages. Special Session on Quantum Computing at the Twenty-second Conference on the Mathematical Foundations of Programming Semantics, 2006, Genova.

[12] Rohit Chadha, Damiano Macedonio, and Vladimiro Sassone. A hybrid intuitionistic logic: Semantics and decidability. *International Journal of Logic and Computation (Special issue on Logics for Resources, Processes and Programs)*, 16(1):27–59, 2006. 33 pages.

[13] Rohit Chadha, Steve Kremer, and Andre Scedrov. Formal analysis of multiparty contract signing. *Journal of Automated Reasoning* , 36(1-2):39–83, 2006. 45 pages.

[14] Rohit Chadha, John Mitchell, Andre Scedrov, and Vitaly Shmatikov. Contract signing, optimism and advantage. *Journal of Logic and Algebraic Programming (Special issue on Modeling and Verification of Cryptographic Protocols)*, 64(2):189–218, 2005. 30 pages. Invited submission.

Peer-reviewed conference proceedings

[1] Gergei Bana, Rohit Chadha and Ajay Kumar Eeralla. Formal Analysis of Vote Privacy Using Computationally Complete Symbolic Attacker. In Javier López, Jianying Zhou and Miguel Soriano, editors, 23rd European Symposium on Research in Computer Security (ESORICS), pages 350–372, 2018.

[2] Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan. Approximating Probabilistic Automata by Regular Languages. In Dan R. Ghica and Achim Jung, editors, *27th EACSL Annual Conference on Computer Science Logic (CSL)*, pages 14:1–14:23, 2018.

[3] Matt Bauer, Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan. Model Checking Indistinguishability of Randomized Security Protocols In Hana Chockler and Georg Weissenbacher, editors, *30th International Conference on Computer-Aided Verification (CAV)*, pages 117–135, 2018.

[4] Matt Bauer, Umang Mathur, Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan. Exact Quantitative Model Checking Through Rational Search. In Daryl Stewart and Georg Weissenbacher, editors, *17th International conference on Formal Methods in Computer-Aided Design (FMCAD)*, pages 92–99, 2017.

[5] Matt Bauer, Rohit Chadha and Mahesh Viswanathan. Modular Verification of Protocol Equivalence in the Presence of Randomness. In Dieter Gollman and Simon Foley, editors, *22nd European Symposium on Research in Computer Security (ESORICS)*, pages 1–12, 2017.

[6] Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan. Verification of randomized security protocols. In Joel Ouaknine, editor, *32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. pages 1–12, 2017.

[7] Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan. Emptiness under isolation and the value problem for hierarchical probabilistic automata. In Javier Esparza and Andrzej Murawski, editors, *20th International Conference on Foundations of Software Science and Computation Structures, (FoSSaCS)*, pages 231–247, 2017.

[8] Matt Bauer, Rohit Chadha and Mahesh Viswanathan. Composing protocols with randomized actions. In Frank Piessens and Luca Vigan, editors, *5th International Conference on Principles of Security and Trust (POST)*. Pages 189-210, 2016.

[9] Rohit Chadha, Mahesh Viswanathan, Prasad Sistla and Yue Ben. Decidable and Expressive classes of Probabilistic Automata. In Andrew Pitts, editor, *18th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS)*, pages 200-214, 2015.

[10] Rohit Chadha, Umang Mathur and Stefan Schwoon. Computing information leakage using symbolic model-checking. In Venkatesh Raman and S. P. Suresh, editors, *Annual Conference on Foundations of Software Technology and Theoretical Computer Science, (FST&TCS)*, pages 505-516, 2014.

[11] Rohit Chadha, Dilip Kini and Mahesh Viswanathan. Decidable problems for unary PFAs. In Gethin Norman and William H. Sanders, editors, *11th International Conference on Quantitative Evaluation of Systems (QEST)*, pages 329–344, 2014.

[12] Rohit Chadha, Dileep Kini and Mahesh Viswanathan. Quantitative information flow in Boolean Programs. In Martin Abadi and Steve Kremer, editors, *3rd International Conference on Principles of Security and Trust (POST)*, pages 103-119, 2014.

[13] Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan. Probabilistic Automata with Isolated Cut-Points. In K. Chatterjee and J. Sgall, editors, *38th International Symposium on Mathematical Foundations of Computer Science (MFCS),* volume 8087 of *Lecture Notes in Computer Science*, pages 254-265, 2013. Springer.

[14] Rémi Bonnet and Rohit Chadha. Bounded Context-Switching and Reentrant Locking. In Frank Pfenning, editor, *16th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS),* volume 7794 of *Lecture Notes in Computer Science*, pages 65-80, 2013. Springer.

[15] Rohit Chadha and Michael Ummels. The complexity of information leakage in recursive programs. In Deepak D'Souza, T. Kavitha and Jaikumar Radhakrishnan, editors, *32nd Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS)*, volume 18 of *Leibniz International Proceedings in Informatics*, pages 534–545, 2012. Leibniz-Zentrum fuer Informatik.

[16] Rohit Chadha, P. Madhusudan and M. Viswanathan. Reachability under Contextual Locking. In Cormac Flanagan and Barbara König, editors, *18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 7214 of *Lecture Notes in Computer Science*, pages 437–450, 2012. Springer.

[17] Rohit Chadha, Ştefan Ciobaca and Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. In Helmut Seidl, editor, *22nd European Symposium on Programming (ESOP)*, volume 7211 of *Lecture Notes in Computer Science*, pages 108–127, 2012. Springer.

[18] Rohit Chadha, Vijay Korthikranthi, Mahesh Viswanathan, Gul Agha and Youngmin Kwon. Model Checking MDPs with A Unique Compact Invariant Set of Distributions. In Alma Riska and Catuscia Palamidessi, editors, *Eighth International Conference on Quantitative Evaluation of SysTems (QEST)*, pages 121-130, 2011. IEEE Computer Society.

[19] Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. Probablistic Büchi automata with non-extremal acceptance thresholds. In Ranjit Jhala and David A. Schmidt, editors, *Twelfth International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI)*, pages 103–117, 2011.

[20] Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. Model checking concurrent programs with nondeterminism and randomization. In Kamal Lodaya and Meena Mahajan, editors, *Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS)*, volume 8 of *Leibniz International Proceedings in Informatics*, pages 364–375, 2010. Leibniz-Zentrum für Informatik.

[21] Rohit Chadha, Axel Legay, Pavithra Prabhakar, and Mahesh Viswanathan. Complexity bounds for the verification of real-time software. In Gilles Barthe and Manuel Hermenegildo, editors, *Proceedings of the 11th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI)*, volume 5944 of *Lecture Notes in Computer Science*, pages 95–111, 2010.

[22] Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. Power of randomization in automata on infinite strings. In Mario Bravetti and Gianluigi Zavattaro, editors, *Proceedings of the 20th International Conference on Concurrency Theory (CONCUR)*, volume 5710 of *Lecture Notes in Computer Science*, pages 229–243, Bologna, Italy, 2009.

[23] Rohit Chadha, Stéphanie Delaune, and Steve Kremer. Epistemic logic for the applied pi calculus. In David Lee, Antónia Lopes, and Arnd Poetzsch-Heffter, editors, *Proceedings of IFIP International Conference on Formal Techniques for Distributed Systems (FMOODS/FORTE)*, volume 5522 of *Lecture Notes in Computer Science*, pages 182–197, Lisbon, Portugal, 2009.

[24] Rohit Chadha, Mahesh Viswanathan, and Ramesh Viswanathan. Least upper bounds for probability measures and their applications to abstractions. In Franck van Breugel and Marsha Chechik, editors, *19th International Conference on Concurrency Theory (CONCUR)*, volume 5201 of *Lecture Notes in Computer Science*, pages 264–278, 2008.

[25] Rohit Chadha, A. Prasad Sistla, and Mahesh Viswanathan. On the expressiveness and complexity of randomization in finite state monitors. In *23rd Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 18–29. IEEE Computer Society, 2008.

[26] Rohit Chadha, Carl A. Gunter, Jose Meseguer, Ravinder Shankesi, and Mahesh Viswanathan. Modular preservation of safety properties by cookie-based dos-protection wrappers. In Gilles Barthe and Frank S. de Boer, editors, *10th IFIP WG 6.1 International Conference on Formal Methods for Open Object-Based Distributed Systems (FMOODS)*, volume 5051 of *Lecture Notes in Computer Science*, pages 39–58, 2008.

[27] Rohit Chadha and Mahesh Viswanathan. Decidability results for well-structured transition systems with auxiliary storage. In Luís Caires and Vasco Thudichum Vasconcelos, editors, *18th International Conference on Concurrency Theory (CONCUR)*, volume 4703 of *Lecture Notes in Computer Science*, pages 136–150, 2007.

[28] Pedro Baltazar, Rohit Chadha, Paulo Mateus and Amílcar Sernadas. Towards Model-Checking Quantum Security Protocols In First International Conference on Quantum, Nano, and Micro Technologies (ICQNM), pages 14. IEEE Computer Society, 2007.

[29] Rohit Chadha, Paulo Mateus, and Amilcar Sernadas. Reasoning about states of probabilistic sequential programs. In Zoltán Ésik, editor, *Computer Science Logic, 20th International Workshop (CSL)*, volume 4207 of *Lecture Notes in Computer Science*, pages 240–255, 2006.

[30] Rohit Chadha, Steve Kremer, and Andre Scedrov. Formal analysis of multi-party contract signing. In R. Focardi, editor, *17th IEEE Computer Security Foundations Workshop (CSFW)*, pages 266–279. IEEE Computer Society, 2004.

[31] Rohit Chadha, John Mitchell, Andre Scedrov, and Vitaly Shmatikov. Contract signing, optimism and advantage. In R. Amadio and D. Lugiez, editors, *14th International Conference on Concurrency Theory (CONCUR)*, pages 366–382, 2003.

[32] Rohit Chadha, Max Kanovich, and Andre Scedrov. Inductive methods and contract-signing protocols. In P. Samarati, editor, *8th ACM Conference on Computer and Communications Security (CCS)*, pages 176–185, ACM Press, 2001.

Submitted Papers

[1] Matt Bauer, Umang Mathur, Rohit Chadha, A. Prasad Sistla and Mahesh Viswanathan. Exact quantitative model checking using rational search. Submitted to Formal Methods in System Design.

[2] Rohit Chadha, Dilip Kini, Michael Ummels and Mahesh Viswanathan. The Complexity of Quantitative Information Flow in Programs. Submitted to Information and Computation. Conditionally accepted.

[3] Gergei Bana, Rohit Chadha, Ajay K. Eeralla and M. Okada. Verification Methods for the Computationally Complete Symbolic Attacker Based on Indistinguishability. Submitted to ACM transactions on Computational Logic.

Software Tools

SPAN
Tool for verifying randomized security protocols
`https://github.com/bauer-matthews/SPAN`

RatSearch
Tool for exact modelchecking in DTMCs and MDPs
`https://publish.illinois.edu/rationalmodelchecker`

Moped-QLeak
Tool to estimate information leakage in deterministic and probabilistic programs
`https://github.com/umangm/mopedqleak`

AKiSs
Tool for checking trace equivalence for security protocols
`https://github.com/akiss/akiss`

Invited Talks

1. *Towards verifying randomized cryptographic protocols.* Workshop on Computer Security, Logic, and Programming Languages. Workshop in Honor of John Mitchell's 60th Birthday. May 2016, Stanford University, USA.
2. *Probabilistic models and their analysis.* 16th International Workshop on Verification of Infinite-State Systems (INFINITY 2014) A post-FSTTCS 2014 workshop, December 2014, Indian Institute of Technology, Delhi, India.
3. *Automated verification of equivalence properties of cryptographic protocols.* Summer School on Formal Methods for the Science of Security, July 2013. Information Trust Institute, University of Illinois at Urbana-Champaign Champaign, USA.
4. *Probabilistic Automata with Isolated Cut-Points.* Conference Presentation at MFCS, August 2013, Vienna, Austria.
5. *Bounded Context-Switching and Reentrant Locking.* Conference Presentation at FoSSaCS, March 2013, Rome, Italy.
6. *The Complexity of Quantitative Information Flow in Recursive Programs.* Conference Presentation at FST & TCS, December 2013, Hyderabad, India.

7. *Automated verification of equivalence properties of cryptographic protocols.* University of Illinois at Urbana-Champaign, 2012, Champaign, USA.
8. *Reachability under Contextual Locking.* Conference Presentation at TACAS, March 2012, Tallinn, Estonia.
9. *Automated verification of equivalence properties of cryptographic protocols.* Conference Presentation at ESOP, March 2012, Tallinn, Estonia.
10. *Model Checking MDPs with A Unique Compact Invariant Set of Distributions.* Conference Presentation at QEST, September 2011, Aachen, Germany.
11. *Power of Randomization in Finite State Monitoring.* LaBRI, University of Bordeaux, May 2011, Bordeaux, France.
12. *Power of Randomization in Finite State Monitoring.* University of Technology, April 2011, Sydney, Australia.
13. *Probabilistic Büchi automata with non- extremal acceptance thresholds.* Conference Presentation at VMCAI, January 2011, Austin, USA.
14. *Model checking concurrent programs with nondeterminism and randomization.* Conference Presentation at FST & TCS, December 2010, Chennai, India.
15. *Power of Randomization in Finite State Monitoring.* INRIA Rennes, June 2010, Rennes, France.
16. *Modelchecking Concurrent Programs with Nondeterminism and Randomization.* LIAFA, University Paris Diderot - Paris 7, February 2011, Paris, France.
17. *Modelchecking Concurrent Programs with Nondeterminism and Randomization.* LIX, L'École Polytechnique, December 2010, Palaiseau, France.
18. *Power of Randomization in Finite State Monitoring.* Max-Planck Institute, November 2010, Kaiserlautern, Germany.
19. *Power of Randomization in Finite State Monitoring.* IRISA, University of Rennes, May 2010 Rennes, France.
20. *Least upper bounds for probability measures and their applications to abstractions.* Conference Presentation at CONCUR, August 2008, Toronto, Canada.
21. *On the expressiveness and complexity of randomization in finite state monitors.* Conference Presentation at LICS, June 2008, Pittsburgh, USA.
22. *Modular preservation of safety properties by cookie-based dos-protection wrappers.* Conference Presentation at FMOODS, June 2008, Oslo, Norway.
23. *Decidability results for well-structured transition systems with auxiliary storage.* LSV- CNRS & ENS de Cachan, October 2007, Cachan, France.
24. *Decidability results for well-structured transition systems with auxiliary storage.* LIAFA, University Paris Diderot - Paris 7, October 2007, Paris, France.
25. *Decidability results for well-structured transition systems with auxiliary storage.* Conference Presentation at CONCUR, September 2007, Lisbon, Portugal.
26. *Modular Preservation of Safety Properties by Cookie-Based DoS-Protection Wrappers.* Dagstuhl seminar "Formal Protocol Verification Applied", October 2007. Dagstuhl, Germany.
27. *Formal analysis of multi-party contract signing.* Conference Presentation at CSFW, June 2004, Asilomar, USA.
28. *Formal analysis of multi-party contract signing.* Microsoft Research, February 2004, Cambridge, UK.
29. *Advantage and abuse-freeness in contract-signing protocols.* Special session on Security at the Mathematical Foundations of Programming Semantics, March 2002, New Orleans, USA.

30. *Inductive methods and contract-signing protocols.* Conference Presentation at CCS, November 2001, Philadelphia, USA.

Student advising

Phd Students

- Matt Bauer, Co-advisor, UIUC, 2014-2018. Now at Galois Inc.
- Ajay Kumar Eeralla (2014-present)
- Seth Ahrenbach (2016-present)
- Ali Bajwa (2018-present)

Masters Students

- Jia Chen (2013-2014)
- Vasanthi Manhandi (2015-2016)
- Brandon Splitter (2018-Present)

Undergraduate Research Students

- Elizabeth J. White
- Adam Faszl
- Umang Mathur (INRIA)

Teaching Experience

Lecturer, Spring 2017
Cryptography and Formal Proofs
Department of Electrical Engineering and Computer Science, University of Missouri
Proposed and designed the course

Lecturer, Fall 2012, Spring 2015, Spring 2016, Spring 2018
Formal Engineering Methods for Software and Security
Department of Computer Science, University of Missouri
Proposed and designed the course

Lecturer, Fall 2014, Spring 2015, Fall 2015, Fall 2016, Fall 2017
Advanced Algorithm Design, Part I
Department of Computer Science, University of Missouri

Lecturer, Spring 2012, Fall 2014, Fall 2016, Fall 2017
Introduction to Cryptography
Department of Computer Science, University of Missouri
Proposed and designed the course

Lecturer, Spring 2014
Theory of Compilers
Department of Computer Science, University of Missouri

Lecturer, Fall 2013
Principles of Programming Languages
Department of Computer Science, University of Missouri

Probabilistic Aspects in Computer Science Course, 2010 and 2011
Parisian Master of Research in Computer Science, France
Proposed and designed the case

Course co-designer, Fall 2008
Dept. of Computer Science, Univ. of Illinois, Urbana-Champaign
Co-designed the course "Logical Foundations of Computer Science"

Professional Duties

Refereeing duties

- Grant Proposal Reviewer, NSF Panel, 2013 and 2018
- Grant Proposal Reviewer, UM Research Board Proposal Reviewers, 2014 and 2016
- Program Committee Member
  - 30th International Conference on Computer-Aided Verification (CAV), 2018
  - Young Researchers Workshop on Concurrency Theory (YR-CONCUR), 2017
  - 15th International Symposium on Automated Technology for Verification and Analysis (ATVA), 2017
  - 29th International Conference on Computer-Aided Verification (CAV), 2017
  - Quantitative Evaluation of Systems - 13th International Conference (QEST), 2016
  - International Symposium on Digital Forensics and Security, 4th IEEE Conference (ISDFS), 2016
  - 15th International conference on Runtime Verification (RV), 2015.
  - 35th International Conference on Formal Techniques for Distributed Objects, Components and Systems (FORTE), 2015.
  - 3rd IEEE International Workshop on Formal Methods Integration (FMi), 2015
  - 8th International Conference on Information Security Practice and Experience (ISPEC), 2013.
  - Information Security Practice and Experience - 7th International Conference, ISPEC 2012
  - Young Researchers Workshop on Concurrency Theory (YR-CONCUR), 2012
- Frequent reviewer for several international journals and conferences such as
  - Journal of Computer Security (JCS)
  - ACM Transactions on Computational Logic (TOCL)
  - ACM Transactions on Programming Languages and Systems (TOPLAS)
  - Theoretical Computer Science (TCS)
  - ACM Transactions on Information and System Security (TISSEC)
  - Formal methods in System Design (FMSD)
  - Automated Software Engineering (AUSE)
  - Journal of Computer and System Sciences (JCSS)
  - Synthese
  - Journal of the ACM (JACM)
  - Logical methods in Computer Science (LMCS)
  - Mathematical Structures in Computer Science (MSCS)
  - International Colloquium on Automata, Languages and Programming (ICALP)

- International Symposium on Mathematical Foundations of Computer Science (MFCS)
- International Conference on Computer-Aided Verification (CAV)
- Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)
- European Symposium on Programming (ESOP)
- Computer Security Foundations Symposium (CSF)
- International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)
- Foundations of Software Technology and Theoretical Computer Science (FST&TCS)
- Foundations of Software Science and Computation Structures (FoSSaCS)
- International Joint Conference on Automated Reasoning (IJCAR)
- ACM Conference on Computer and Communications Security (CCS)
- Software Engineering and Formal Methods (SEFM)
- International Conference on Concurrency Theory (CONCUR)

Summer School Lecture

Invited lecture at Summer School on Formal Methods for the Science of Security. Information Trust Institute, University of Illinois at Urbana-Champaign (UIUC), 2013

Committee Duties

- College of Engineering Honors Committee Department of Electrical Engineering and Computer Science, 2018-Present
- College of Engineering Scholarship Committee, Department of Electrical Engineering and Computer Science, 2017-Present
- Graduate Curriculum Committee, 2017- Present, Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, USA
- High Assurance Cyberphysical Systems Search Sub-Committee, Department of Electrical Engineering and Computer Science, 2017
- Undergraduate Curriculum Committee, 2012- 2016, Department of Computer Science, University of Missouri, Columbia, USA
- Non-Tenure Track Faculty Search Committee, 2016, Department of Computer Science, 2016
- Steering committee, Midwest Verification Day, 2014-2016
- Student Financial Aid Committee, 2013- 2015, University of Missouri, Columbia, USA
- Co-organizer, Security reading group, 2013-2014, Department of Computer Science, University of Missouri, Columbia, USA
- Member of Scientific Policy Committee, 2010-2011, Laboratoire Spécification et Vérification, CNRS & ENS de Cachan, France
- Departmental Seminar Organizer, 2010-2011, Laboratoire Spécification et Vérification, CNRS & ENS de Cachan, France

Workshop organization

Midwest Verification Day, October 3-4, 2014, University of Missouri, Columbia

References

Somesh Jha
Computer Sciences Department, Univ. of Wisconsin Madison
Email: jha@cs.wisc.edu

Andre Scedrov
Department of Mathematics, Univ. of Pennsylvania
Email: scedrov@math.upenn.edu

Vitaly Shmatikov
Department of Computer Science, Cornell Tech
Email: shmat@cs.cornell.edu

Mahesh Viswanathan
Department of Computer Science, Univ. of Illinois
Email: vmahesh@cs.uiuc.edu