397, Engineering 2, UC Santa Cruz,
1156 High Street, Santa Cruz, CA 95064.
✉ vasundar@ucsc.edu
http://vaishs.github.io

Vaishnavi Sundararajan

❉ Education & Employment

Nov 2020–	**Postdoctoral Scholar**, *University of California, Santa Cruz.*
Jan 2020–Oct 2020	**Research Associate**, *Ericsson Research, Bengaluru.*
Nov 2018–Oct 2019	**Postdoctoral Researcher**, *CNRS, IRISA Rennes.*
2012–2018	**PhD, Computer Science**, *Chennai Mathematical Institute*, Degree conferred July 2019.
2010–2011	**MSE, Computer Science and Engineering**, *University of Michigan, Ann Arbor*, 7.0/9.0.
2006–2010	**BE, Instrumentation & Control Engineering**, *Delhi University*, 77% (First with distinction).

❉ Research Interests

Formal methods and verification, logic, proof theory, security protocols

❉ Programming Skills/Tools Known

Languages:	Haskell, OCaml, C++, Java, PHP/SQL
Tools:	Coq, Tamarin, Scyther, Proverif, CBMC, Isabelle

❉ Publications

Authors	Alexandrous Nikou*, Anusha Mujumdar*, Vaishnavi Sundararajan*, Marin Orlic, Aneta Vulgarakis Feljan
Title	"Safe RAN Control: A Symbolic Reinforcement Learning Approach"
To appear in	*International Conference of Control and Automation (ICCA)*, 2022.
Authors	Karl Norrman, Vaishnavi Sundararajan, Alessandro Bruni †
Title	"Formal Analysis of EDHOC Key Establishment for Constrained IoT Devices"
Published in	*Proc. SECRYPT 2021, ISBN 978-989-758-524-1*, pages 210–221, DOI: 10.5220/0010554002100221, 2021.
Authors	David Fernández-Duque, Hans van Ditmarsch, Vaishnavi Sundararajan, S P Suresh
Title	"Who holds the best card? Secure communication of optimal secret bits"
Published in	*Australasian Journal of Combinatorics, 80*, pages 1–29, 2021.
Authors	Véronique Cortier, Stéphanie Delaune, Vaishnavi Sundararajan
Title	"A decidable class of security protocols for both reachability and equivalence properties"
Published in	*Journal of Automated Reasoning, 65*, pages 479–520, DOI:10.1007/s10817-020-09582-9, 2021.
Authors	R Ramanujam, Vaishnavi Sundararajan, S P Suresh
Title	"The complexity of disjunction in intuitionistic logic"
Published in	*Journal of Logic and Computation, 30(1)*, pages 421–445, DOI:10.1093/logcom/exaa018, 2020.
Author	Vaishnavi Sundararajan
Title	"A theory of assertions for Dolev-Yao models"
	PhD Thesis, 2018. https://www.dropbox.com/s/bg11nuohpfnhjdy/thesis.pdf
Authors	R Ramanujam, Vaishnavi Sundararajan, S P Suresh
Title	"Existential assertions for voting protocols"
Published in	*Proc. FC 2017, LNCS volume 10323*, pages 337–352, DOI: 10.1007/978-3-319-70278-0_21, 2017.

∗ Joint primary contributors † Names in order of contribution

Authors	R Ramanujam, Vaishnavi Sundararajan, S P Suresh
Title	"The complexity of disjunction in intuitionistic logic"
Published in	*Proc. LFCS 2016, LNCS volume 9537*, pages 349–363, DOI: 10.1007/978-3-319-27683-0_24, 2016.
Authors	R Ramanujam, Vaishnavi Sundararajan, S P Suresh
Title	"Extending Dolev-Yao with assertions"
Published in	*Proc. ICISS 2014, LNCS volume 8880*, pages 50–68, DOI: 10.1007/978-3-319-13841-1_4, 2014.
Authors	Saurabh Bharadwaj, Smriti Srivastava, S Vaishnavi, J R P Gupta †
Title	"Chaotic time series prediction using combination of Hidden Markov Model & Neural Nets"
Published in	*Proc. CISIM 2010*, pp.585–589, DOI: 10.1109/CISIM.2010.5643518, 2010.
Authors	Anand Gupta, S Vaishnavi, Saurav Malviya †
Title	"Time-efficient dynamic scene management using octrees"
Published in	*Proc. IEEE INMIC 2008*, pp.111–115, DOI: 10.1109/INMIC.2008.4777718, 2008.

❉ Technical Reports

Authors	R Ramanujam, Vaishnavi Sundararajan, S P Suresh
Title	"Protocol insecurity with assertions" https://arxiv.org/abs/2202.04518 (Under submission)
Authors	Kristijonas Cyras, Ramamurthy Badrinath, Swarup Kumar Mohalik, Anusha Mujumdar, Alexandros Nikou, Alessandro Previti, Vaishnavi Sundararajan, Aneta Vulgarakis Feljan
Title	"Machine reasoning explainability" https://arxiv.org/abs/2009.00418

❉ Outreach and Professional Activities

PC Member	Student Research Competition, PLDI 2022
Reviewer	The Computer Journal, Oxford University Press (2021)
Mentor	MINT Community, Womxn's Centre, UC Santa Cruz (2021–present)
Mentor	UMIAA (2019–2020)
Member	Google Women Techmakers (2016–present)

❉ Awards

2014–2018	Infosys Foundation Grant
2013–2018	TCS Research Scholarship
2014	Second-best Paper Award, ICISS 2014
2011	Finalist, Google Anita Borg Memorial Scholarship (USA)

❉ Talks

June 2019 **Poster presentation and 5-minute talk (CSF 2019)**, *"Deciding trace equivalence for protocols with asymmetric operations"*.
CSF 2019, Hoboken, NJ, USA.

May 2019 **Research presentation (FMAI 2019)**, *"Who holds the best card? Secure communication of optimal secret bits"* (Co-presented with Hans van Ditmarsch).
FMAI 2019, IRISA, Rennes, France.

March 2019 **Invited talk**, *"A theory of assertions for Dolev-Yao models"*.
LaBRI, Bordeaux, France.

December 2018 **Research presentation (5èmes Journées MAFTEC 2018)**, *"Who holds the best card? Secure communication of optimal secret bits"* (Co-presented with Hans van Ditmarsch).
MAFTEC 2018, IRISA, Rennes, France.

October 2018 **Invited talk (SRM-ACM Student Chapter camp on Cybersecurity and Cryptography)**, *"Keeping secrets in the digital age"*.
SRM Institute of Science and Technology, Chennai, India.

July 2018 **Research presentation**, *"A theory of assertions for Dolev-Yao models"*.
FM Update Meeting 2018. Goa, India.

July 2018 **Invited talk**, *"A theory of assertions for Dolev-Yao models"*.
Tata Research Development and Design Centre, Pune, India.

June 2018 **Invited talk**, *"A theory of assertions for Dolev-Yao models"*.
IRISA, Rennes, France.

March 2018 **Invited talk**, *"Formal verification of security protocols"*.
SRM Institute of Science and Technology, Chennai, India.

June 2016 **Invited talk**, *"Extending Dolev-Yao with assertions"*.
LORIA, Nancy, France.

March 2015 **Invited talk**, *"Extending Dolev-Yao with assertions"*.
The Institute of Mathematical Sciences, Chennai, India.

July 2013 **Research presentation**, *"From LTL to deterministic omega-automata"*.
FM Update Meeting 2013, Delhi, India.

❉ Experience

Jan–Jun 2020 **Co-supervisor (with Dr. Swarup Kumar Mohalik)**, *Ericsson Research*, Bengaluru.
Co-supervised Mr. Swarnadeep Bhattacharya, ISI Kolkata, during his six-month internship on "Towards automating the formal verification of security protocols".
Introduced concepts of formal verification and security protocols, and guided the student while he implemented a parser to convert arrow notation input into a protocol based on roles, variables etc.

Aug–Dec 2017 **Co-instructor (with Prof. S P Suresh)**, *Chennai Mathematical Institute*, Chennai.
Taught a course on Formal Methods for Cryptographic Protocols.
Gave lectures, helped set and grade assignments and exams.

June 2016 **Co-instructor (with Prof. S P Suresh)**, *Vellore Institute of Technology*, Vellore.
Taught a course on security protocol design and verification as part of the ACM Summer School on Information and Systems Security. Introduced the Dolev-Yao model, and presented general ideas about hiding information from non-malicious agents using zero-knowledge proofs etc.

September 2016 **Co-instructor (with Prof. S P Suresh)**, *NIE Mysore*, Mysore.
Taught an introductory course on functional programming using Haskell.

Jan–April 2015 **Teaching Assistant**, *Chennai Mathematical Institute*, Chennai.
TA for Programming Language Concepts. Prof. S P Suresh.
Helped set and grade assignments and exams.

Aug–Dec 2014 **Teaching Assistant**, *Chennai Mathematical Institute*, Chennai.
TA for Programming in Haskell. Prof. S P Suresh.
Helped set and grade assignments and exams.

2012–2013 **Research Assistant**, *Chennai Mathematical Institute*, Chennai.
RA for a project funded by the Defence Research and Development Organization, India.
Developed a toolkit to be used by non-experts for cryptographic protocol verification, to translate protocol descriptions and some simple properties from the Alice-Bob arrow format to the syntax of some known tool. Explored various tools – Scyther, Proverif and Isabelle. Shared the design and programming responsibilities for the toolkit.

Aug–Dec 2011 **Graduate Student Instructor**, *University of Michigan*, Ann Arbor.
GSI for EECS 376: Foundations of Computer Science. Prof. Kevin Compton.
Conducted discussion sessions and held office hours.

Jan–April 2011 **Graduate Student Instructor**, *University of Michigan*, Ann Arbor.
GSI for EECS 487: Interactive Computer Graphics. Prof. Sugih Jamin.
Held office hours and conducted lab sessions.