Vaishnavi Sundararajan

✉ vasundar@ucsc.edu
http://cmi.ac.in/~vaishnavi

❉ Education & Employment

Nov 2020–	**Research 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:	Tamarin, Scyther, Proverif, CBMC, Isabelle

❉ Publications

Authors	Karl Norrman, Vaishnavi Sundararajan, Alessandro Bruni †
Title	"Formal Analysis of EDHOC Key Establishment for Constrained IoT Devices"
	Accepted at SECRYPT 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, 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, 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 Workshops (Voting 2017), Springer LNCS volume 10323*, pages 337–352, 2017.
Authors	R Ramanujam, Vaishnavi Sundararajan, S P Suresh
Title	"The complexity of disjunction in intuitionistic logic"
Published in	*Proc. LFCS 2016, Springer LNCS volume 9537*, pages 349–363, 2016.
Authors	R Ramanujam, Vaishnavi Sundararajan, S P Suresh
Title	"Extending Dolev-Yao with assertions"

Last updated: June 1, 2021

† Names in order of contribution

Published in	*Proc. ICISS 2014, Springer LNCS volume 8880*, pages 50–68, 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, 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, 2008.

❉ 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

December 2019	**Invited talk**, *"A gentle introduction to formally verifying security protocols"*. Ericsson Research, Bengaluru, India.
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.
August 2018	**Thesis defense**, *"A theory of assertions for Dolev-Yao models"*. Chennai Mathematical Institute, 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.
April 2017	**Paper presentation (FC 2017)**, *"Existential assertions for voting protocols"*. FC 2017 (Voting Workshop), Sliema, Malta.
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.

December 2014 **Paper presentation (ICISS 2014)**, *"Extending Dolev-Yao with assertions"*.
ICISS 2014, IDRBT, Hyderabad, India.

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

❉ Experience

Jan–Jun 2020 **Internship co-supervisor**, *Ericsson Research*, Bengaluru.
Co-supervised (along with Dr. Swarup Kumar Mohalik) 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**, *Chennai Mathematical Institute*, Chennai.
Taught (along with Prof. S P Suresh) a course on Formal Methods for Cryptographic Protocols.
Gave lectures, helped set and grade assignments and exams.

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

September 2016 **Co-instructor**, *NIE Mysore*, Mysore.
Taught (along with Prof. S P Suresh) an introductory course on functional programming, by invitation at NIE Mysore.
Helped students write programs in 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.
The aim of the project was to develop a toolkit to be used by non-experts for cryptographic protocol verification. The toolkit would be used 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. Also helped the professor set the homeworks and exams, and grade the course.

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. Also set homeworks and helped the professor set exams and grade the course.