Vaishnavi Sundararajan

Postdoctoral Researcher, University of California Santa Cruz

vasundar@ucsc.edu | vaishs.github.io | gGJ7qxUAAAAJ | vaishnavi-srajan

Experience

UNIVERSITY OF CALIFORNIA SANTA CRUZ

Postdoctoral Researcher — Nov 2020 – Current | Santa Cruz, USA

- Extending FLAFOL with operators for belief, equality, and Fitch-style implication.
- Using choreographies to bring secure-by-construction information-flow reasoning to concurrent programs.

ERICSSON RESEARCH

Research Associate — Jan 2020 – Oct 2020 | Bengaluru, India

- Worked on the verification of the EDHOC protocol.
- Co-supervised the intern Mr. Swarnadeep Bhattacharya.
- Worked on the safe Reinforcement Learning project.
- Co-wrote the report on explainability and MR.
- Discussed formal methods for neural networks and RL.

CNRS, IRISA, RENNES

Postdoctoral Researcher — Nov 2018 – Oct 2019 | Rennes, France

- Worked on obtaining decidability results for trace and equivalence properties for a class of security protocols.
- Wrote an OCaml tool that checked this membership.

Research Interests

• Formal methods • Verification • Security protocols • AI/ML

Skills

Programming: • Haskell • OCaml • Python • Java • C/C++
Tools: • Coq • Tamarin • Proverif • CBMC • Isabelle

Education

CHENNAI MATHEMATICAL INSTITUTE

PhD in Computer Science
Thesis: A Theory of Assertions for Dolev-Yao Models
Defended: Aug 2018 Degree Conferred: July 2019

UNIVERSITY OF MICHIGAN ANN ARBOR

MSE in Computer Science and Engineering
Aug 2010 – Dec 2011 7.0 / 9.0

NETAJI SUBHAS INSTITUTE OF TECHNOLOGY, DELHI UNIVERSITY

BE in Instrumentation & Control Engineering
Aug 2006 – June 2010 77%, First with distinction

Awards

2022	Recipient	Best Paper, ICCA
2014–2018	Recipient	Infosys Foundation Grant
2014–2018	Recipient	TCS Research Scholarship
2014	Recipient	Second Best Paper, ICISS
2011	Finalist	Anita Borg Scholarship (USA)

Activities and Outreach

- PC Member, PLDI SRC 2022
- Member, UCSC WiSE Program (2022–present)
- Mentor, UCSC MINT Program (2021–present)
- Mentor, UMIAA (2019–2020)

Publications

[Equal contributions unless indicated otherwise by superscripts]

Alexandrous Nikou[1], Anusha Mujumdar[1], Vaishnavi Sundararajan[1], Marin Orlic[2], Aneta Vulgarakis Feljan[2]. Safe RAN Control: A Symbolic Reinforcement Learning Approach. To appear in ICCA 2022.

Karl Norrman[1], Vaishnavi Sundararajan[2], Alessandro Bruni[3]. Formal Analysis of EDHOC Key Establishment for Constrained IoT Devices. Proc. SECRYPT 2021, ISBN 978-989-758-524-1, pages 210–221, 2021.

David Fernández-Duque, Hans van Ditmarsch, Vaishnavi Sundararajan, S P Suresh. Who Holds the Best Card? Secure Communication of Optimal Secret Bits. Australasian Journal of Combinatorics, 80, pages 1–29, 2021.

Véronique Cortier, Stéphanie Delaune, Vaishnavi Sundararajan. A Decidable Class of Security Protocols for both Reachability and Equivalence Properties. Journal of Automated Reasoning, 65, pages 479–520, 2021.

R Ramanujam, Vaishnavi Sundararajan, S P Suresh. The Complexity of Disjunction in Intuitionistic Logic. Journal of Logic and Computation, 30(1), pages 421–445, 2020.

R Ramanujam, Vaishnavi Sundararajan, S P Suresh. Existential Assertions for Voting Protocols. Proc. FC 2017, LNCS volume 10323, pages 337–352, 2017.

R Ramanujam, Vaishnavi Sundararajan, S P Suresh. The Complexity of Disjunction in Intuitionistic Logic. Proc. LFCS 2016, LNCS volume 9537, pages 349–363, 2016.

R Ramanujam, Vaishnavi Sundararajan, S P Suresh. Extending Dolev-Yao with Assertions.
Proc. ICISS 2014, LNCS volume 8880, PAGES 50–68, 2014.

Saurabh Bharadwaj[1], Smriti Srivastava[2], S Vaishnavi[3], J R P Gupta[4]. Chaotic Time Series Prediction using Combination of Hidden Markov Model & Neural Nets. Proc. CISIM 2010, PAGES 585–589, 2010.

Anand Gupta[1], S Vaishnavi[2], Saurav Malviya[3]. Time-Efficient Dynamic Scene Management using Octrees.
Proc. IEEE INMIC 2008, PAGES 111–115, 2008.

Teaching and Research Experience

Introduction to Introduction to Programming Workshop: Instructor, online. June 2022–July 2022.
Introduced the fundamental concepts of programming (via an interactive online workshop focused on problem solving) to participants at UC Santa Cruz from non-computer science backgrounds who have no coding knowledge.

Internship Co-supervisor (with Dr. Swarup Kumar Mohalik), Ericsson Research, Bengaluru. Jan–Jun 2020.
Co-supervised Mr. Swarnadeep Bhattacharya during his internship. Introduced concepts of formal verification and security protocols, and guided him while he implemented a parser to convert Alice-Bob input into a formal protocol.

Formal Methods for Cryptographic Protocols: Co-instructor (with Prof. S P Suresh), CMI, Chennai. Aug–Dec 2017.
Gave lectures, helped set and grade assignments and exams.

Security Protocols (Design & Verification): Co-instructor (with Prof. S P Suresh), VIT, Vellore. June 2016.
Taught a course on security protocols as part of the ACM Summer School on Information and Systems Security. Introduced the Dolev-Yao model, and presented ideas about hiding information using zero-knowledge proofs &c.

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

Programming Language Concepts: TA for Prof. S P Suresh, CMI, Chennai. Jan–April 2015.
Helped set and grade assignments and exams.

Programming in Haskell: TA for Prof. S P Suresh, CMI, Chennai. Aug–Dec 2014.
Helped set and grade assignments and exams.

DRDO Project, Research Assistant, CMI, Chennai. 2012–2013.
Worked with Prof. S P Suresh on a project funded by the Defence Research and Development Organization, India. Developed a toolkit to be used for cryptographic protocol verification, to translate protocol descriptions and some simple properties from the Alice-Bob arrow format to the syntax of tools like Scyther, Proverif and Isabelle.

Foundations of Computer Science: TA for Prof. Kevin Compton, University of Michigan, Ann Arbor. Aug–Dec 2011.
Conducted discussion sessions, held office hours, and helped set and grade assignments and exams.

Interactive Computer Graphics: TA for Prof. Sugih Jamin, University of Michigan, Ann Arbor. Jan–April 2011.
Conducted lab sessions and held office hours, and helped set and grade assignments and exams.

Selected Invited Talks

Invited talk. LSD Seminar, October 2021, UC Santa Cruz. Better Safe than Sorry: Symbolic Verification for Security Protocols

Research presentation (Co-presented with Hans van Ditmarsch). FMAI 2019, IRISA, Rennes.
Who Holds the Best Card? Secure Communication of Optimal Secret Bits

Invited talk. Seminaire M2F, March 2019, LaBRI, Bordeaux. A Theory of Assertions for Dolev-Yao Models

Research presentation (Co-presented with Hans van Ditmarsch). 5èmes Journées MAFTEC 2018, IRISA, Rennes.
Who Holds the Best Card? Secure Communication of Optimal Secret Bits

Invited talk. ACM Student Chapter camp on Cybersecurity and Cryptography, October 2018, SRM, Chennai.
Keeping Secrets in the Digital Age

Invited talk. March 2018, SRM, Chennai. Formal Verification of Security Protocols

Invited talk. June 2016, LORIA, Nancy. Extending Dolev-Yao with Assertions