Vaishnavi Sundararajan

Assistant Professor, Department of Computer Science & Engineering, IIT Delhi

vaishnavi@cse.iitd.ac.in | vaishs.github.io | Ysw8fq4AAAAJ | 011-26591292

Experience

INDIAN INSTITUTE OF TECHNOLOGY
Assistant Professor — Apr 2023 – present | New Delhi, India

- Also associated with the Centre of Excellence in Cyber Systems and Information Assurance (CSIA)

CHENNAI MATHEMATICAL INSTITUTE
Postdoctoral Researcher — Jan 2023 – Mar 2023 | Chennai, India

- Worked on the active intruder problem for assertions.

UNIVERSITY OF CALIFORNIA SANTA CRUZ
Postdoctoral Researcher — Nov 2020 – Oct 2022 | Santa Cruz, USA

- Extended FLAFOL with operators for belief, equality &c.
- Worked on 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

Education

CHENNAI MATHEMATICAL INSTITUTE
PhD in Computer Science
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, ISEC 2023
- PC Member, PLDI SRC 2022
- Member, UCSC WiSE Program (2022–present)
- Mentor, UCSC MINT Program (2021–present)
- Mentor, UMIAA (2019–2020)

Skills

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

Publications

[Equal contributions unless indicated otherwise by superscripts]

R Ramanujam, Vaishnavi Sundararajan, S P Suresh. Protocol Insecurity with Assertions. https://arxiv.org/abs/2308.13773, 2023.

Karl Norrman[1], Vaishnavi Sundararajan[2], Alessandro Bruni[1]. Extended Formal Analysis of the EDHOC Protocol in Tamarin. E-Business and Telecommunications, Communications in Computer and Information Science, volume 1795, pages 224–248, 2023.

Alexandrous Nikou[1], Anusha Mujumdar[1], Vaishnavi Sundararajan[1], Marin Orlic[2], Aneta Vulgarakis Feljan[2]. Safe RAN Control: A Symbolic Reinforcement Learning Approach. Proc. ICCA 2022, ISBN 978-166-549-573-8, pages 332–337 , 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, ISSN 2202-3518, volume 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 Experience

COL876 Special Topics in Formal Methods: Instructor, IIT Delhi. July 2023–present.
Teaching the fundamentals of symbolic verification of security protocols, and how to use tools to automate the same.

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 from non-computer science backgrounds with no prior 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.

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

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.

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.

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

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

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