

# Vaishnavi Sundararajan

Chandruka New Faculty Fellow & Assistant Professor, Department of CSE, IIT Delhi

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

## EXPERIENCE

### INDIAN INSTITUTE OF TECHNOLOGY DELHI

ASSISTANT PROFESSOR Apr 2023 – present | New Delhi, India

- ✦ Chandruka New Faculty Fellow
- ✦ 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 • Logic • Verification • Security

## EDUCATION

### CHENNAI MATHEMATICAL INSTITUTE

PHD IN COMPUTER SCIENCE

### UNIVERSITY OF MICHIGAN ANN ARBOR

MSE IN COMPUTER SCIENCE AND ENGINEERING

### NETAJI SUBHAS INSTITUTE OF TECHNOLOGY, DELHI UNIVERSITY

BE IN INSTRUMENTATION & CONTROL ENGINEERING

## AWARDS

- |      |   |
|------|---|
| 2023 | Chandruka New Faculty Fellowship, IIT Delhi   |
| 2023 | Young Faculty Incentive Fellowship, IIT Delhi |
| 2022 | Best Paper, ICCA                              |
| 2014 | Infosys Foundation Grant                      |
| 2014 | TCS Research Scholarship                      |
| 2014 | Second Best Paper, ICISS                      |

## ACTIVITIES AND OUTREACH

- **PC Member:** OOPSLA 2025, ISEC 2025, ICLA 2025, ACM India ARCS 2025 (Area chair: Theory), ICISS 2024, ISEC 2024, PLDI SRC 2022
- **Organizer:** Winter School on Theory, IIT Delhi 2023
- **Mentor:** UCSC MINT Program (2021–2022)

## PUBLICATIONS

[EQUAL CONTRIBUTIONS UNLESS INDICATED OTHERWISE BY SUPERSSCRIPTS]

R Ramanujam, Vaishnavi Sundararajan, S P Suresh. Solving the Insecurity Problem for Assertions. Proc. 37th IEEE Computer Security Foundations Symposium (CSF'24), PAGES 636–650, 2024.

Karl Norrman<sup>1</sup>, Vaishnavi Sundararajan<sup>2</sup>, Alessandro Bruni<sup>1</sup>. 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<sup>1</sup>, Anusha Mujumdar<sup>1</sup>, Vaishnavi Sundararajan<sup>1</sup>, Marin Orlic<sup>2</sup>, Aneta Vulgarakis Feljan<sup>2</sup>. Safe RAN Control: A Symbolic Reinforcement Learning Approach. Proc. ICCA 2022, ISBN 978-166-549-573-8, PAGES 332–337, 2022.

Karl Norrman<sup>1</sup>, Vaishnavi Sundararajan<sup>2</sup>, Alessandro Bruni<sup>3</sup>. Formal Analysis of EDHOC Key Establishment for Constrained IoT Devices. Proc. SECURE 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<sup>1</sup>, Smriti Srivastava<sup>2</sup>, S Vaishnavi<sup>3</sup>, J R P Gupta<sup>4</sup>. Chaotic Time Series Prediction using Combination of Hidden Markov Model & Neural Nets. Proc. CISIM 2010, PAGES 585–589, 2010.

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

---

## TEACHING EXPERIENCE

COL703 Logic in Computer Science: Instructor, IIT Delhi. July 2024–present.

Teaching various logics (propositional, first-order etc) with a view to their use in Computer Science.

COL226 Programming Languages: Co-Instructor (with Prof. Sanjiva Prasad), IIT Delhi. Jan 2024–May 2024.

Taught various aspects of the foundations of programming languages.

COL876 Special Topics in Formal Methods: Instructor, IIT Delhi. July 2023–Dec 2023.

Taught 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. Logic & AI seminar, June 2024, University of Bergen. Formally Verifying Security Protocols with Certification

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, May 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