Ajith Suresh

PostDoc. · Research Scholar

ENCRYPTO, Department of Computer Science of Technical University of Darmstadt, Germany

(+49) 1625122156 | suresh@encrypto.cs.tu-darmstadt.de | www.ajithsuresh.github.io | ajithsuresh | @Ajith_Suresh92 | Ajith Suresh

"Be weird. Be random. Be who you are. Because you never know who would love the person you hide."

Research Interests

My research focuses on cryptography and information security, emphasising efficient and secure protocols for problems in the area of Multi-party Computation (MPC). My current focus is on MPC for privacy-preserving services on the internet and in the area of Machine Learning and Federated Learning. The topics of cryptography I have been interested in so far include MPC, Verifiable Secret Sharing, Oblivious Transfer, Byzantine Agreement and Broadcast, Privacy-Preserving Machine Learning and Federated Learning.

Education

Indian Institute of Science (IISc) — *Bengaluru, India*

Ph. D. in Computer Science — *Sep. 2017 - Jul. 2021*

- Dissertation Area: Secure Multi-party Computation (MPC) & Privacy-Preserving Machine Learning (PPML)
- Dissertation Title: MPCLeague: Robust MPC Platform for Privacy-Preserving Machine Learning
- Advisor: Prof. Arpita Patra
- CGPA: 9 / 10 (First Class with Distinction)

Indian Institute of Science (IISc) — *Bengaluru, India*

M.Tech. (Research) in Computer Science — *Aug. 2014 - Jun. 2017*

- Dissertation Area: Secure Multi-party Computation (MPC)
- Dissertation Title: Fast Actively Secure OT Extension for Short Secrets
- Advisor: Prof. Arpita Patra
- CGPA: 6.83 / 8 (First Class with Distinction)

College of Engineering, Trivandrum (CET) — *Trivandrum, India*

B.Tech in Computer Science and Engineering — *Jul. 2010 - Apr. 2014*

- Thesis Title: Proximity-based Sentiment Analysis with Contextual Phrase Polarity
- CGPA: 8.81 / 10 (First Class with Distinction)

Professional Experience

Technical University (TU) of Darmstadt — *Darmstadt, Germany*

Post-Doctoral Research in Computer Science — *Oct. 2021 - Present*

- Area: Privacy-preserving Services On the Internet (PSOTI)
- Host: Prof. Thomas Schneider
- Research Group: Cryptography and Privacy Engineering (ENCRYPTO)

Indian Institute of Science (IISc) — *Bengaluru, India*

Research Associate — *Aug. 2021 - Sep. 2021*

- Research associate under the guidance of Arpita Patra.

Technical University (TU) of Darmstadt — *Darmstadt, Germany*

Research Intern — *Nov. 2019*

- Research work under the joint guidance of Thomas Schneider and Arpita Patra.
- The project aimed at improving the efficiency of secure two-party computation.
- Resulted in a publication at USENIX Security Symposium'21.

Amazon Development Centre — *Bangalore, India*

Software Development Engineer (SDE) Intern — *Jul. 2013 - Aug. 2013*

- Worked on the project titled "Increase the registered and subscribed user base at Amazon" under the mentorship of Bhanu Pratap Singh in the International Expansion (Junglee Traffic) Team.

Awards, Scholarships and Achievements

1. Nominated for the Schmidt Science Fellows 2022 program for post-doctoral research (one among a group of 350 highly accomplished candidates, nominated from 83 of the world's leading universities and institutes).
2. Represented country India in the "Window to the World" session at the 8th Heidelberg Laureate Forum.
3. Selected as one among 225 young researchers to participate in the 8th Heidelberg Laureate Forum.
4. Recipient of Google PhD Fellowship 2019 (one among 53 researchers around the globe).
5. Organiser of Secure Multi-Party Computation: Theory and Practice Workshop at Indian Institute of Science (IISc) from 19th to 22nd January, 2020.
6. Received travel grant to attend Privacy Preserving Machine Learning Workshop, CCS 2019, London.
7. Received travel grant to attend Workshop: Theory and Practice of Secure Multiparty Computation 2016, Aarhus University, Denmark.
8. Secured All India Rank of 807 with a score of 688 in GATE 2014 among (approximately) 1,55,190 students in India.
9. Ministry of Human Resource and Development (MHRD) Scholarship for Postgraduate education, India.
10. Best Outgoing student in Computer Science and Engineering (P Rathnaswamy Memorial Endowment) for the year 2014.
11. First prize in Coding Competition, CODESTORM, conducted by IEEE Computer Society (March 2013).
12. Received Ashok Leyland "ALL THE BEST" Scholarship for graduate studies, India (February 2011).
13. Recipient of Federal Bank Hormis Memorial Foundation Scholarship for graduate studies, India (2010-11).
14. Recipient of Indian Oil Education Scholarship for graduate education, India (2010-11).
15. Received Central Sector Scholarship by Department of Higher Education (MHRD) for graduate studies, India (2010).
16. Achieved a rank of 629 in Kerala Engineering Entrance (KEAM 2010) among (approximately) 100949 students.
17. Received Malayala Manorama Merit Scholarship (February 2008).
18. Received prize at CMS Math Prodigy Hunt 2009, organized by Centre for Research in Mathematics.
19. Participated in 20th Kerala Science Congress, Trivandrum (January 2008).
20. Participated in Youth Parliament Competition under the auspices of the Institute of Parliamentary Affairs, Government of Kerala.

Skills

Programming	C/C++, Java, Javascript, Python, PyTorch
DevOps	AWS, Docker
DBMS	Oracle, SQL
Web	HTML5, CSS3, jQuery, JSP
Tools	NetBeans, Eclipse, LaTeX

Personal Data

Born	24th April 1992 in Kerala, India
Citizenship	Indian
Marital Status	Married
Languages	Malayalam (mother tongue), English, Hindi, Tamil
Interests	Photography, Badminton, Cycling