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. 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.

Education

Indian Institute of Science (IISc)

Bengaluru, India

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

- Specialization: Secure Multi-party Computation (MPC)
- Thesis Title: MPCLeague: Robust MPC Platform for Privacy-Preserving Machine Learning
- Advisor: Prof. Arpita Patra
- Research Group: Cryptography and Information Security (CrIS)
- CGPA: 9 / 10 (First Class with Distinction)

Indian Institute of Science (IISc)

Bengaluru, India

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

- Specialization: Secure Multi-party Computation (MPC)
- Thesis Title: Fast Actively Secure OT Extension for Short Secrets
- Advisor: Prof. Arpita Patra
- Research Group: Cryptography and Information Security (CrIS)
- 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

Germany

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

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

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 work titled"ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation" which got accepted to 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.

Publications

Publications in cryptography usually order authors alphabetically (using surnames) and conferences are more common than journals. I am the primary author for publications marked with †.

1. Nishat Koti, Arpita Patra, Rahul Rachuri and Ajith Suresh. *Tetrad: Actively Secure 4PC for Secure Training and Inference*†. In 29th Network and Distributed System Security Symposium (NDSS'22) (CORE rank- A*)
   Full version: `ia.cr/2021/755`
2. Arpita Patra, Thomas Schneider, Ajith Suresh and Hossein Yalame. *SynCirc: Efficient Synthesis of Depth-Optimized Circuits for Secure Computation*. In IEEE International Symposium on Hardware Oriented Security and Trust (HOST'21)
   Full version: `ia.cr/2021/1153`
3. Nishat Koti, Mahak Pancholi, Arpita Patra and Ajith Suresh. *SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning*†. In 30th USENIX Security Symposium (USENIX'21) (CORE rank- A*)
   Full version: `ia.cr/2020/592`
4. Arpita Patra, Thomas Schneider, Ajith Suresh and Hossein Yalame. *ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation*†. In 30th USENIX Security Symposium (USENIX'21) (CORE rank- A*)
   Full version: `ia.cr/2020/1225`
5. Arpita Patra and Ajith Suresh. *BLAZE: Blazing Fast Privacy-Preserving Machine Learning*†. In 27th Network and Distributed System Security Symposium (NDSS'20) (CORE rank- A*)
   Full version: `ia.cr/2020/042`
6. Harsh Chaudhari, Rahul Rachuri and Ajith Suresh. *Trident: Efficient 4PC Framework for Privacy Preserving Machine Learning*†. In 27th Network and Distributed System Security Symposium (NDSS'20) (CORE rank- A*)
   Full version: `ia.cr/2019/1315`
7. Megha Byali, Harsh Chaudhari, Arpita Patra and Ajith Suresh. *FLASH: Fast and Robust Framework for Privacy-preserving Machine Learning*. In 20th Privacy Enhancing Technologies Symposium (PETS'20) (CORE rank- A)
   Full version: `ia.cr/2019/1365`
8. Harsh Chaudhari, Ashish Choudhury, Arpita Patra and Ajith Suresh. *ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction*†. In ACM Conference on Cloud Computing Security Workshop (ACM CCSW'19)
   Full version: `ia.cr/2019/429`
9. Arpita Patra, Pratik Sarkar and Ajith Suresh. *Fast Actively Secure OT Extension for Short Secrets*†. In 24th Network and Distributed System Security Symposium (NDSS'17) (CORE rank- A*)
   Full version: `ia.cr/2016/940`

Workshops / Posters

1. Nishat Koti, Shravani Patil, Arpita Patra and Ajith Suresh.. *MPClan: Protocol Suite for Privacy-Conscious Computations*. In NDSS'22 (Poster)
2. Nishat Koti, Arpita Patra, Rahul Rachuri and Ajith Suresh. *Tetrad: Actively Secure 4PC for Secure Training and Inference*. In PPML'21 (ACM CCS'21)
   Full version: `ia.cr/2021/755`
3. Arpita Patra, Thomas Schneider, Ajith Suresh and Hossein Yalame. *ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation*. In PriML'21 (NeurIPS'21), In PPML'21 (ACM CCS'21), In PPML'21 (CRYPTO'21)
   Full version: `ia.cr/2020/1225`
4. Nishat Koti, Arpita Patra and Ajith Suresh. *MPCLeague: Robust and Efficient Mixed-protocol Framework for 4-party Computation*. In IEEE S&P'21 (Poster), In DPML'21 (ICLR'21)
   Poster: `https://www.ieee-security.org/TC/SP2021/downloads/poster/poster25.pdf`
   Full version: `dp-ml.github.io/2021-workshop-ICLR/files/9.pdf`
5. Nishat Koti, Mahak Pancholi, Arpita Patra and Ajith Suresh. *SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning*. In ARCS'22 (Symposium), In DPML'21 (ICLR'21), In PriML/PPML'20 (NeurIPS'20)
   Full version: `ia.cr/2020/592`
6. Harsh Chaudhari, Ashish Choudhury, Arpita Patra and Ajith Suresh. *ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction*. In PPML'19 (ACM CCS'19)
   Full version: `ia.cr/2019/429`

Preprints

1. Nishat Koti, Shravani Patil, Arpita Patra and Ajith Suresh. *MPClan: Protocol Suite for Privacy-Conscious Computations*. Under Submission

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.

Talks and Presentations

1. August 2021. *SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning*. 30th USENIX Security Symposium, Virtual Event.
2. June 2021. *SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning*. CNI Networks Seminar Series, Centre for Networked Intelligence, Virtual Event, India.
3. May 2021. *MPC for small population with applications to Privacy-Preserving Machine Learning*. EECS Research Students Symposium 2021, Virtual Event, India.
4. May 2021. *MPCLeague: Robust and Efficient Mixed-protocol Framework for 4-party Computation*. Distributed and Private Machine Learning (DPML), ICLR Workshop 2021, Virtual Event.
5. February 2021. *ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation*. 15th Academic Research and Careers for Students Symposium (ARCS) 2021, Virtual Event, India.
6. February 2021. *BLAZE: Blazing Fast Privacy-Preserving Machine Learning*. 15th Academic Research and Careers for Students Symposium (ARCS) 2021, Virtual Event, India.

7. July 2020. *MPC MEETS ML: Efficient Privacy Preserving Machine Learning Techniques*. EECS Research Students Symposium 2020, Virtual Event, India.
8. July 2020. *MPC MEETS ML: Efficient Privacy Preserving Machine Learning Techniques*. International Symposium on Current Trends in Research and Innovation (ISCTRI'20), Virtual Event, india.
9. February 2020. *BLAZE: Blazing Fast Privacy-Preserving Machine Learning*. The Network and Distributed System Security Symposium (NDSS) 2020, San Diego, USA.
10. February 2020. *Trident: Efficient 4PC Framework for Privacy Preserving Machine Learning*. The Network and Distributed System Security Symposium (NDSS) 2020, San Diego, USA.
11. February 2020. *ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction*. 14th Inter-Research-Institute Student Seminar in Computer Science (IRISS) 2020, IIT Gandhinagar.
12. January 2020. *MPC MEETS ML: Efficient Privacy Preserving Machine Learning Techniques*. Hitachi-IISc Project Review, IISc, India.
13. January 2020. *MPC MEETS ML: Efficient Privacy Preserving Machine Learning Techniques*. Secure Multi-Party Computation: Theory and Practice Workshop, IISc, India.
14. November 2019. *ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction*. TU Darmstadt, Germany.
15. March 2019. *MPC MEETS ML: High Throughput Secure ML Prediction*. Amazon Project Review, IISc, India.
16. August 2018. *Cryptography Basics*. QIP STC on Foundations of Cryptography, IISc, India.
17. April 2017. *Fast Actively Secure OT Extension for Short Secrets*. EECS Symposium, IISc, India.
18. February 2017. *Fast Actively Secure OT Extension for Short Secrets*. The Network and Distributed System Security Symposium (NDSS) 2017, San Diego, USA.
19. February 2016. *Oblivious Transfer (OT) and OT Extensions*. Workshops on Cryptography, organized as a part of Information Security Education and Awareness Project Phase II, IISc.
20. February 2016. *Two party computation (GMW construction)*. Workshops on Cryptography, organized as a part of Information Security Education and Awareness Project Phase II, IISc.
21. February 2016. *Message Authentication Codes*. Workshops on Cryptography, organized as a part of Information Security Education and Awareness Project Phase II, IISc.
22. January 2016. *Efficient Actively Secure Oblivious Transfer Extension*. 10th Inter-Research-Institute Student Seminar in Computer Science (IRISS) 2016, Technopark, Trivandrum, Kerala.

Research Events

1. August 2021. 8th Heidelberg Laureate Forum. Heidelberg (Virtual Event), Germany.
2. August 2021. The 30th USENIX Security Symposium (USENIX) 2021. (Virtual Event).
3. May 2021. EECS Research Students Symposium 2021. Indian Institute of Science (IISc), Bangalore (Virtual Event), India.
4. May 2021. Distributed and Private Machine Learning (DPML), ICLR Workshop 2021. (Virtual Event).
5. February 2021. 15th Academic Research and Careers for Students Symposium (ARCS) 2021. PSG College of Technology, Coimbatore (Virtual Event), India.
6. July 2020. EECS Research Students Symposium 2020. Indian Institute of Science (IISc), Bangalore (Virtual Event), India.
7. July 2020. International Symposium on Current Trends in Research and Innovation (ISCTRI'20). CHRIST University, Pune Lavasa Campus (Virtual Event), India.
8. February 2020. The 27th Network and Distributed System Security Symposium (NDSS) 2020. San Diego, USA.
9. February 2020. 14th Inter-Research-Institute Student Seminar in Computer Science (IRISS) 2020. Indian Institute of Technology (IIT) Gandhinagar, India.
10. January 2020. Secure Multi-Party Computation : Theory and Practice 2020. Indian Institute of Science (IISc), Bangalore, India.
11. November 2019. The 26th ACM Conference on Computer and Communications Security (CCS) 2019. London, United Kingdom.
12. December 2017. 18th International Conference on Cryptology (INDOCRYPT) 2017. The Institute of Mathematical Sciences (IMSc), Chennai, India.

13. March 2017. NMI Workshop on Secure Multiparty Computation. Indian Institute of Technology (IIT), Bomaby, India.
14. February 2017. The 24th Network and Distributed System Security Symposium (NDSS) 2017. San Diego, USA.
15. June 2016. Theory and Practice of Secure Multiparty Computation Workshop (TPMPC) 2016. Aarhus university, Denmark.
16. January 2016. 10th Inter-Research-Institute Student Seminar in Computer Science (IRISS) 2016. Trivandrum, India.

Scientific Service

1. Acted as *external reviewer* for
    - 2022 - EUROCRYPT, ACM CCS, IEEE TDSC (Journal)
    - 2021 - ACM CCS, PODC, ITC, CRYPTO
    - 2020 - ASIACRYPT, IEEE TIFS (Journal)
    - 2019 - CRYPTO, ASIACRYPT, TCC, PKC
    - 2018 - EUROCRYPT, ASIACRYPT
    - 2017 - ASIACRYPT, PKC
    - 2016 - CRYPTO
2. Organiser of EECS Research Students Symposium 2017 at Indian Institute of Science (IISc), Bangalore, India.

Teaching Experience

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

CSA E0 312 : Secure Computation (Teaching Assistant) *Jan. - Apr.'17, Aug. - Dec.'19*

- Instructor: Dr. Arpita Patra
- Department of Computer Science and Automation (CSA), IISc.
- Gave course lectures, mentoring in course projects, evaluation.

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

CSA E0 235 : Cryptography (Teaching Assistant) *Jan. - Apr.'16, Aug. - Dec.'19*

- Instructor: Dr. Arpita Patra
- Department of Computer Science and Automation (CSA), IISc.
- Conducted weekly tutorial sessions discussing questions from the areas covered in the course, evaluation of exam sheets.

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

UG E101 : Algorithms and Programming (Teaching Assistant) *Aug. - Dec.'18*

- Instructors: Satish Govindarajan and Viraj Kumar
- Undergraduate (UG) Department , IISc.
- Conducted weekly coding tutorial sessions, evaluation of assignments.

Projects

College of Engineering, Trivandrum *Trivandrum, India*

BTech Main Project *Jan. - Mar.'14,*

- Title: Proximity based Sentiment Analysis with Contextual Phrase Polarity.
- This aims to find the sentiment or mood of a given text segment (or review) using word proximity.

College of Engineering, Trivandrum *Trivandrum, India*

BTech Mini Project *Jan.'13,*

- Title: Student Tracker - A complete student management system.
- A tool for managing the student database of a college using Java front end and Oracle back end.

College of Engineering, Trivandrum *Trivandrum, India*

Other Projects

- A project on Road Safety using mobile controlled speed governor in association with IEEE.
- A project on android device that can convert a base line video to normal high quality video for live streaming, in association with IET and Aceware Technology Ltd.

Skills

Programming	C/C++, Java, Javascript, Python
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