Ajith Suresh

Contact Information

Department of Computer Science & Automation,
Indian Institute Of Science (IISc), Bangalore,
Bengaluru, India - 560012
ajith@iisc.ac.in, ajith424suresh@gmail.com
https://www.csa.iisc.ac.in/ cris/ajith

Koppara Veedu
Kalayapuram P.O
Kollam, Kerala
India - 691560
+918762049224

Research Interests

My research focuses on cryptography and information security, with emphasis on finding efficient and secure protocols for problems in the area of Multi-party Computation (MPC). My current focus is on MPC for small population and it's application to the area of Privacy Preserving 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), Bangalore

Ph.D., Computer Science — September 2017 to present

- Specialization: *MPC for small population with applications to Privacy Preserving Machine Learning*
- Advisor: Dr. Arpita Patra
- CGPA : 9/10

Indian Institute Of Science (IISc), Bangalore

M.Tech (Research), Computer Science — June 2017

- Specialization: *Cryptography (Multi-party Computation)*
- Thesis Title: *Fast Actively Secure OT Extension for Short Secrets*
- Advisor: Dr. Arpita Patra
- CGPA : 6.83/8

College Of Engineering (CET), Trivandrum, Kerala, India

Bachelor of Technology (B. Tech), Computer Science — April 2014

- Thesis Title: *Proximity based Sentiment Analysis with Contextual Phrase Polarity*
- CGPA : 8.81/10

SN Trust's HSS, Kollam, Kerala, India

Higher Secondary Education (12th) — April 2010

- Percentage : 96.67 %

SVMMHSS, Vendar, Kerala, India

SSLC (10th) — March 2008

- Percentage : 98.89 %

Preprints

- Privacy Preserving Machine Learning[1]
  - *TRISHUL: Efficient Mixed Protocol Framework For Privacy Preserving Machine Learning.* Authors: Arpita Patra and **Ajith Suresh**. (Under preparation)
  - *Bridge: Practically Efficient 3PC Mixed World Framework for Privacy Preserving Machine Learning.* Authors: Nishat Koti, Shravani Patil, Arpita Patra and **Ajith Suresh**. (Under preparation)
  - *ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation.* Authors: Arpita Patra, Thomas Schneider, **Ajith Suresh** and Hossein Yalame. (Under submission)

[1] I am the primary contributor for the papers with my name in bold face

- *MPCLeague: Robust and Efficient Mixed-protocol Framework for 4-party Computation.* Authors: Nishat Koti, Arpita Patra and Ajith Suresh. (Under submission)
- *SWIFT: Making BLAZE Great Again.* Authors: Nishat Koti, Mahak Pancholi, Arpita Patra and **Ajith Suresh**.[PDF] (Under submission)

Publications

- Privacy Preserving Machine Learning[2]
  - *BLAZE: Blazing Fast Privacy-Preserving Machine Learning.* Authors: Arpita Patra and **Ajith Suresh**. NDSS 2020.[PDF]
  - *Trident: Efficient 4PC Framework for Privacy Preserving Machine Learning.* Authors: Harsh Chaudhari, Rahul Rachuri and **Ajith Suresh**. NDSS 2020.[PDF]
  - *FLASH: Fast and Robust Framework for Privacy-preserving Machine Learning.* Authors: Megha Byali, Harsh Chaudhari, Arpita Patra and Ajith Suresh. PETS 2020.[PDF]
  - *ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction.* Authors: Harsh Chaudhari, Ashish Choudhury, Arpita Patra and **Ajith Suresh**. ACM CCSW 2019, PPML 2019.[PDF]
- Oblivious Transfer and Extensions
  - *Fast Actively Secure OT Extension for Short Secrets.* Authors: Arpita Patra, Pratik Sarkar and **Ajith Suresh**. NDSS 2017.[PDF]

Awards, Scholarships and Achievements

- Selected as one among 225 young researchers to participate in the 8th Heidelberg Laureate Forum.
- Recipient of Google PhD Fellowship 2019.
- Organiser of Secure Multi-Party Computation: Theory and Practice Workshop at Indian Institute of Science (IISc) from 19^{th} to 22^{nd} January, 2020.
- Received travel grant to attend Privacy Preserving Machine Learning Workshop, CCS 2019, London.
- Received travel grant to attend Workshop: Theory and Practice of Secure Multiparty Computation 2016, Aarhus University, Denmark.
- Secured All India Rank of 807 with a score of 688 in GATE 2014 among (approximately) 1,55,190 students in India.
- Ministry of Human Resource and Development (MHRD) Scholarship for Postgraduate education, India.
- Best Outgoing student in Computer Science and Engineering (P Rathnaswamy Memorial Endowment) for the year 2013-2014 May 2014
- First prize in Coding Competition, CODESTORM, conducted by IEEE Computer Society March 2013
- Achieved a rank of 629 in Kerala Engineering Entrance (KEAM) in the year 2010 among (approximately) 100949 students in India.
- Received Malayala Manorama Merit Scholarship February 2008.
- Received prizes at Science Fair conducted in inter-school level.
- Received prize at CMS Math Prodigy Hunt 2009, organized by Centre for Research in Mathematics, January 2009.
- Participated in 20th Kerala Science Congress, Trivandrum January 2008.
- Participated in Youth Parliament Competition under the auspices of the Institute of Parliamentary Affairs, Government of Kerala.

[2] I am the primary contributor for the papers with my name in bold face

Talks and Presentations

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

Teaching Experience

Teaching Assistant — Jan–Apr'17, Aug–Dec'19
CSA E0 312 : Secure Computation
Instructor: Dr. Arpita Patra
Department of Computer Science and Automation, IISc
– Tutorial sessions discussing questions from the areas covered in the course, Evaluation of exam sheets.

Teaching Assistant — Jan–Apr'16, Aug-Dec'19
CSA E0 235 : Cryptography
Instructor: Dr. Arpita Patra
Department of Computer Science and Automation, IISc
– Tutorial sessions discussing questions from the areas covered in the course, Evaluation of exam sheets.

Coursework During Ph.D.

– Blockchain and Its Applications
– Graph Theory
– Topics in Advanced Cryptography

Coursework During M.Tech (Research)

– Secure Computation
– Cryptography
– Automata Theory
– Discrete Mathematics
– Algorithms & Approximation Algorithms

Work Experience

Software Development Engineer Intern — July – August 2013
Amazon Development Centre, Bangalore, India
Guide: Bhanu Pratap Singh
International Expansion (Junglee Traffic) Team
Project Title : *Increase the registered and subscribed user base at Amazon.*

Academic Projects Undertaken During BTech

Main Project : — January - March 2014
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.

Mini Project : — January 2013
Title : *Student Tracker*
– A tool for managing the student database of a college using Java front end and Oracle back end.

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.

Software Skills

Programming Languages:
– C/C++, Java, Javascript, Python

Database Management Systems:
– Oracle, SQL

Web:
– HTML, CSS, jQuery, JSP

Tools:
– NetBeans, Eclipse, LaTeX

Additional Information

Strengths
- A good team player.
- Strong Commitment and dedication towards work
- Willingness to learn.
- Positive attitude towards life.

Mother Tongue:
– Malayalam

Other languages:
– English, Hindi, Tamil

Personal Interests
– Photography, Badminton, Chess

LinkedIn Profile
– in.linkedin.com/in/ajithsuresh/