Ajith Suresh

Senior MPC Researcher

Technology Innovation Institute (TII), Abu Dhabi

(+971) 505077924 | ajith.suresh@tii.ae | 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 primarily centers on cryptography and information security, with a special emphasis on creating efficient protocols for problems in the area of Secure Multi-party Computation (MPC). My work revolves around designing and implementing practical MPC protocols, as well as delving into the realms of privacy-preserving machine learning and federated learning. I have actively engaged in a diverse range of cryptographic areas, including Multi-party Computation, Verifiable Secret Sharing, Oblivious Transfer, Byzantine Agreement, Broadcast, as well as cutting-edge domains like 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)
- 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)
- 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*

- CGPA: 8.81 / 10 (First Class with Distinction)

Professional Experience

Technology Innovation Institute (TII) — *Abu Dhabi, UAE*

Senior MPC Researcher — *May. 2023 - Present*

- Secure Multiparty Computation, Privacy-preserving Machine Learning

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

Post-Doctoral Research in Computer Science — *Oct. 2021 - Mar. 2023*

- 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. Received Runner-Up Distinguished Paper Award at 2nd IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML'24).
2. Awarded commendation certificate for outstanding PhD thesis by Department of Computer Science and Automation at the Indian Institute of Science (IISc), Bangalore.
3. 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).
4. Represented country India in the "Window to the World" session at the 8th Heidelberg Laureate Forum.
5. Selected as one among 225 young researchers to participate in the 8th Heidelberg Laureate Forum.
6. Recipient of Google PhD Fellowship 2019 (one among 53 researchers around the globe).
7. Organiser of Secure Multi-Party Computation: Theory and Practice Workshop at Indian Institute of Science (IISc) from 19th to 22nd January, 2020.
8. Received travel grant to attend Privacy Preserving Machine Learning Workshop, CCS 2019, London.
9. Received travel grant to attend Workshop: Theory and Practice of Secure Multiparty Computation 2016, Aarhus University, Denmark.
10. Secured All India Rank of 807 with a score of 688 in GATE 2014 among (approximately) 1,55,190 students in India.
11. Ministry of Human Resource and Development (MHRD) Scholarship for Postgraduate education, India.
12. Best Outgoing student in Computer Science and Engineering (P Rathnaswamy Memorial Endowment) for the year 2014.
13. First prize in Coding Competition, CODESTORM, conducted by IEEE Computer Society (March 2013).
14. Received Ashok Leyland "ALL THE BEST" Scholarship for graduate studies, India (February 2011).
15. Recipient of Federal Bank Hormis Memorial Foundation Scholarship for graduate studies, India (2010-11).
16. Recipient of Indian Oil Education Scholarship for graduate education, India (2010-11).
17. Received Central Sector Scholarship by Department of Higher Education (MHRD) for graduate studies, India (2010).
18. Achieved a rank of 629 in Kerala Engineering Entrance (KEAM 2010) among (approximately) 100949 students.
19. Received Malayala Manorama Merit Scholarship (February 2008).
20. Received prize at CMS Math Prodigy Hunt 2009, organized by Centre for Research in Mathematics.
21. Participated in 20th Kerala Science Congress, Trivandrum (January 2008).
22. Participated in Youth Parliament Competition under the auspices of the Institute of Parliamentary Affairs, Government of Kerala.

Scientific Service

1. *Program Committee* (PC) member for
   - 2026 - PETS
   - 2025 - PETS, IEEE SaTML, ACM CCS, TPMPC, Latincrypt
   - 2024 - IEEE S&P, PETS, TPMPC, WPES (ACM CCS)
   - 2023 - ACM CCS, CANS
   - 2022 - CANS
2. Acted as *external reviewer* for
   - 2024 - EUROCRYPT, CT-RSA, IEEE TDSC, IEEE TIFS
   - 2023 - USENIX Security, CRYPTO
   - 2022 - EUROCRYPT, ACM CCS, PETS, IEEE TDSC, ICDCN, PINS, IEEE TC
   - 2021 - ACM CCS, PODC, ITC, CRYPTO
   - 2020 - ASIACRYPT, IEEE TIFS
   - 2019 - CRYPTO, ASIACRYPT, TCC, PKC
   - 2018 - EUROCRYPT, ASIACRYPT
   - 2017 - ASIACRYPT, PKC
   - 2016 - CRYPTO
3. Organiser of EECS Research Students Symposium 2017 at Indian Institute of Science (IISc), Bangalore, India.
4. Maintainer of https://mpc-deadlines.github.io.

Teaching Experience

Technical University of Darmstadt (TUD) *Darmstadt, Germany*

CRYPROT: Cryptographic Protocols (Teaching Assistant) *Summer Term 2022*

- Instructor: Prof. Dr.-Ing. Thomas Schneider
- ENCRYPTO, Department of Computer Science, TUD.
- Conducted course exercises, exam preparation and evaluation.

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.

Skills

Programming	C/C++, Java, Javascript, Python, PyTorch
DevOps	AWS, Docker, Jenkins, Jira, SonarQube
DBMS	Oracle, SQL
Web	HTML5, CSS3, jQuery, JSP
Tools	NetBeans, Eclipse, VS Code, 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
Contact	Email: ajith424suresh@proton.me, Mob.: (+91) 8762049224

Research Profile

Scientific Publications

Thesis

1. Ajith Suresh. *MPCLeague: Robust MPC Platform for Privacy-Preserving Machine Learning*. PhD Thesis, 2021. Under the supervision of Prof. Arpita Patra. Indian Institute of Science (IISc), Bangalore. [PDF]
2. Ajith Suresh. *Fast Actively Secure OT Extension for Short Secrets*. Master Thesis, 2017. Under the supervision of Prof. Arpita Patra. Indian Institute of Science (IISc), Bangalore. [PDF]
3. Ajith Suresh. *Proximity-based Sentiment Analysis with Contextual Phrase Polarity*. Bachelor Thesis, 2014. College of Engineering (CET), Trivandrum.

Books ([B]) & Book Chapters ([BC])

1. [BC] Najwa Aaraj, Abdelrahaman Aly, Alvaro Garcia-Banda, Chiara Marcolla, Victor Sucasas and Ajith Suresh. *Privacy-Preserving Machine Learning for Massive IoT Deployments*. In Security and Privacy for 6G Massive IoT [PDF]

Conferences ([C]) & Journals ([J])

Publications in cryptography usually order authors alphabetically (using surnames) and conferences ([C]) are more common than journals ([J]). Workshops and affiliated events with proceedings ([W]) are marked with ‡.

1. [J] Daniel Günther, Marco Holz, Benjamin Judkewitz, Helen Möllering, Benny Pinkas, Thomas Schneider and Ajith Suresh. *Privacy-Preserving Epidemiological Modeling on Mobile Graphs*. In IEEE Transactions on Information Forensics & Security (IEEE TIFS'25) (CORE rank- A) [PDF]
2. [J] Najwa Aaraj, Abdelrahaman Aly, Tim Güneysu, Chiara Marcolla, Johannes Mono, Rogerio Paludo, Iván Santos-González, Mireia Scholz, Eduardo Soria-Vazquez, Victor Sucasas and Ajith Suresh. *FANNG-MPC: Framework for Artificial Neural Networks and Generic MPC*. In IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES'25)(CORE rank- A) [PDF]
3. [J] Christopher Harth-Kitzerow, Ajith Suresh, Yonqing Wang, Hossein Yalame, Georg Carle and Murali Annavaram. *High-Throughput Secure Multiparty Computation with an Honest Majority in Various Network Settings*. In 25th Privacy Enhancing Technologies Symposium (PETS'25)(CORE rank- A) [PDF]
4. [C] Yaniv Ben-Itzhak, Helen Möllering, Benny Pinkas, Thomas Schneider, Ajith Suresh, Oleksandr Tkachenko, Shay Vargaftik, Christian Weinert, Hossein Yalame and Avishay Yanai. *ScionFL: Efficient and Robust Secure Quantized Aggregation*. (Runner-Up Distinguished Paper Award) In 2nd IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML'24) [PDF] [Video]
5. [J] Vinod Ganapathy, Eikansh Gupta, Arpita Patra, Gokulnath Pillai and Ajith Suresh. *Privadome: Delivery Drones and Citizen Privacy*. In 24th Privacy Enhancing Technologies Symposium (PETS'24) (CORE rank- A) [PDF]
6. [C] Andreas Brüggemann, Oliver Schick, Thomas Schneider, Ajith Suresh and Hossein Yalame. *Don't Eject the Impostor: Fast Three-Party Computation With a Known Cheater*. In 45th IEEE Symposium on Security and Privacy (IEEE S&P'24) (CORE rank- A*) [PDF] [Video]
7. [C] Gowri R Chandran, Raine Nieminen, Thomas Schneider and Ajith Suresh. *PrivMail: A Privacy-Preserving Framework for Secure Emails*. In 28th European Symposium on Research in Computer Security (ESORICS'23) (CORE rank- A) [PDF]
8. [J] Nishat Koti, Shravani Patil, Arpita Patra and Ajith Suresh. *MPClan: Protocol Suite for Privacy-Conscious Computations*. In Journal of Cryptology (JoC'23) (CORE rank- A*) [PDF]
9. [C] Andreas Brüggemann, Robin Hundt, Thomas Schneider, Ajith Suresh and Hossein Yalame. *FLUTE: Fast and Secure Lookup Table Evaluations*. In 44th IEEE Symposium on Security and Privacy (IEEE S&P'23) (CORE rank- A*) [PDF] [Video]
10. [W] Till Gehlhar, Felix Marx, Thomas Schneider, Ajith Suresh, Tobias Wehrle and Hossein Yalame. *SafeFL: MPC-friendly framework for Private and Robust Federated Learning*‡. In 6th Deep Learning Security and Privacy Workshop (DLSP'23) [PDF]

11. [J] Thomas Schneider, Ajith Suresh and Hossein Yalame.
Comments on "Privacy-Enhanced Federated Learning Against Poisoning Adversaries".
In IEEE Transactions on Information Forensics & Security (IEEE TIFS'23) (CORE rank- A),
In IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'23) [PDF]

Research work(s) published during PhD. I am the primary author for publications marked with †.

12. [C] 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*) [PDF] [Video]
13. [C] 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) [PDF]
14. [C] 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*) [PDF] [Video]
15. [C] 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*) [PDF] [Video]
16. [C] 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*) [PDF] [Video]
17. [C] 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*) [PDF]
18. [J] 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) [PDF] [Video]
19. [C] 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) [PDF]

Research work(s) published during M.Tech. (Research). I am the primary author for publications marked with †.

20. [C] 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*) [PDF] [Video]

Workshops, Symposiums & Posters

1. Abdelrahaman Aly, Sri Harsha Gajavalli, Saurav Pawar, Eduardo Soria-Vazquez, Victor Sucasas and Ajith Suresh.
PetalGuard: Private Federated Learning Framework for Large Language Models.
In Flower AI Summit'25 (Contibuted Talk)
2. Christopher Harth-Kitzerow, Ajith Suresh, Yonqing Wang, Hossein Yalame, Georg Carle and Murali Annavaram.
High-Throughput Secure Multiparty Computation with an Honest Majority in Various Network Settings.
In TPMPC'25 (Contibuted Talk) [PDF]
3. Soumyadyuti Ghosh, Boyapally Harishma, Ajith Suresh, Arpita Patra, Soumyajit Dey, and Debdeep Mukhopadhyay.
Stable and Accurate Real-Time Pricing in Smart Grids.
In TPMPC'25 (Contibuted Talk)
4. Andreas Brüggemann, Oliver Schick, Thomas Schneider, Ajith Suresh and Hossein Yalame.
Don't Eject the Impostor - Honest-Majority MPC With Fixed Malicious Parties.
In TPMPC'25 (Contibuted Talk) [PDF]
5. Najwa Aaraj, Abdelrahaman Aly, Tim Güneysu, Chiara Marcolla, Johannes Mono, Rogerio Paludo, Iván Santos-González, Mireia Scholz, Eduardo Soria-Vazquez, Victor Sucasas and Ajith Suresh.
FANNG-MPC: Framework for Artificial Neural Networks and Generic MPC.
In TPMPC'24 (Contibuted Talk) [PDF] [P] [Video]

6. Andreas Brüggemann, Thomas Schneider, Ajith Suresh and Hossein Yalame.
Is Everyone Equally Trustworthy in Practice? (Short Talk).
In IEEE S&P'23 (Short Talk) []

7. Gowri R Chandran, Raine Nieminen, Thomas Schneider and Ajith Suresh.
PrivMail: A Privacy-Preserving Framework for Secure Emails (Short Talk).
In IEEE S&P'23 (Short Talk) []

8. Andreas Brüggemann, Thomas Schneider, Ajith Suresh and Hossein Yalame.
Efficient Three-Party Shuffling Using Precomputation.
In ACM CCS'22 (Poster) []

9. Daniel Günther, Marco Holz, Benjamin Judkewitz, Helen Möllering, Benny Pinkas, Thomas Schneider and Ajith Suresh.
Privacy-Preserving Epidemiological Modeling on Mobile Graphs.
In ACM CCS'22 (Poster)[] []

10. Nishat Koti, Shravani Patil, Arpita Patra and Ajith Suresh.
MPClan: Protocol Suite for Privacy-Conscious Computations.
In ACM CCS'22 (Poster) [], In NDSS'22 (Poster) []

11. Ajith Suresh.
MPCLeague: Robust MPC Platform for Privacy-Preserving Machine Learning.
In Doctoral Symposium (AIMLSystems'22) [PDF]

12. Nishat Koti, Arpita Patra, Rahul Rachuri and Ajith Suresh.
Tetrad: Actively Secure 4PC for Secure Training and Inference.
In PPML'21 (ACM CCS'21) []

13. 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) []

14. 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) [] []

15. 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) []

16. 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) []

Preprints & Manuscripts

1. Christopher Harth-Kitzerow, Ajith Suresh and Georg Carle.
Truncation Untangled: Scaling Fixed-Point Arithmetic for Privacy-Preserving Machine Learning to Large Models and Datasets.
Under Submission []

2. Felix Marx, Thomas Schneider, Ajith Suresh, Tobias Wehrle, Christian Weinert and Hossein Yalame.
WW-FL: Secure and Private Large-Scale Federated Learning.
Under Submission []

3. Arpita Patra, Joachim Schmidt, Thomas Schneider, Ajith Suresh and Hossein Yalame.
SynCirc: Efficient Synthesis of Depth-Optimized Circuits from High-Level Languages.
Under Submission

4. Soumyadyuti Ghosh, Boyapally Harishma, Ajith Suresh, Arpita Patra, Soumyajit Dey, and Debdeep Mukhopadhyay.
Precision and Privacy: Advancing Real-Time Pricing in Smart Grids with Secure Computation.
Under Submission

Invited Talks

1. March 2025. *MPC-based PPML: Advancing Privacy-Preserving Machine Learning*. MOZAIK Winter School. Leuven, Belgium.
2. March 2025. *Truncation Untangled: Scaling Fixed-Point Arithmetic for Privacy-Preserving Machine Learning to Large Models and Datasets*. COSIC Seminar Series. Leuven, Belgium.
3. November 2024. *Revitalizing Privacy-Preserving Machine Learning: Introducing FANNG-MPC for Actively Secure MLaaS*. CarbyneStackCon'24 (CSC'24). Hybrid Event.
4. June 2021. *SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning*. CNI Networks Seminar Series, Centre for Networked Intelligence, Virtual Event, India.
5. 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.
6. November 2019. *ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction*. TU Darmstadt, Germany.

Other Talks and Presentations

1. June 2024. *Revitalizing Privacy-Preserving Machine Learning: Introducing FANNG-MPC for Actively Secure MLaaS*. 10. Theory and Practice of Multi-Party Computation Workshop (TPMPC 2024). Darmstadt, Germany.
2. April 2024. *ScionFL: Efficient and Robust Secure Quantized Aggregation*. 2nd IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML'24). Toronto, Canada.
3. October 2022. *MPCLeague: Robust MPC Platform for Privacy-Preserving Machine Learning*. Second International Conference on AI-ML Systems (AIMLSystems'22). Bangalore (Hybrid Event), India.
4. April 2022. *Tetrad: Actively Secure 4PC for Secure Training and Inference*. The Network and Distributed System Security Symposium (NDSS) 2022, Hybrid Event.
5. August 2021. *SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning*. 30th USENIX Security Symposium, Virtual Event.
6. May 2021. *MPC for small population with applications to Privacy-Preserving Machine Learning*. EECS Research Students Symposium 2021, Virtual Event, India.
7. May 2021. *MPCLeague: Robust and Efficient Mixed-protocol Framework for 4-party Computation*. Distributed and Private Machine Learning (DPML), ICLR Workshop 2021, Virtual Event.
8. February 2021. *ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation*. 15th Academic Research and Careers for Students Symposium (ARCS) 2021, Virtual Event, India.
9. February 2021. *BLAZE: Blazing Fast Privacy-Preserving Machine Learning*. 15th Academic Research and Careers for Students Symposium (ARCS) 2021, Virtual Event, India.
10. July 2020. *MPC MEETS ML: Efficient Privacy Preserving Machine Learning Techniques*. EECS Research Students Symposium 2020, Virtual Event, India.
11. February 2020. *BLAZE: Blazing Fast Privacy-Preserving Machine Learning*. The Network and Distributed System Security Symposium (NDSS) 2020, San Diego, USA.
12. February 2020. *Trident: Efficient 4PC Framework for Privacy Preserving Machine Learning*. The Network and Distributed System Security Symposium (NDSS) 2020, San Diego, USA.
13. 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.
14. January 2020. *MPC MEETS ML: Efficient Privacy Preserving Machine Learning Techniques*. Hitachi-IISc Project Review, IISc, India.
15. January 2020. *MPC MEETS ML: Efficient Privacy Preserving Machine Learning Techniques*. Secure Multi-Party Computation: Theory and Practice Workshop, IISc, India.
16. March 2019. *MPC MEETS ML: High Throughput Secure ML Prediction*. Amazon Project Review, IISc, India.
17. August 2018. *Cryptography Basics*. QIP STC on Foundations of Cryptography, IISc, India.
18. April 2017. *Fast Actively Secure OT Extension for Short Secrets*. EECS Symposium, IISc, India.
19. February 2017. *Fast Actively Secure OT Extension for Short Secrets*. The Network and Distributed System Security Symposium (NDSS) 2017, San Diego, USA.

20. 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.
21. February 2016. *Two party computation (GMW construction)*. Workshops on Cryptography, organized as a part of Information Security Education and Awareness Project Phase II, IISc.
22. February 2016. *Message Authentication Codes*. Workshops on Cryptography, organized as a part of Information Security Education and Awareness Project Phase II, IISc.
23. 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. March 2025. MOZAIK Winter School. Leuven, Belgium.
2. November 2024. CarbyneStackCon '24 (CSC24). Renningen (Hybrid Event), Germany
3. June 2024. 10. Theory and Practice of Multi-Party Computation Workshop (TPMPC 2024). Darmstadt, Germany.
4. April 2024. 2nd IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML'24). Toronto, Canada.
5. November 2022. The 29th ACM Conference on Computer and Communications Security (CCS). Los Angeles, U.S.A.
6. October 2022. Second International Conference on AI-ML Systems (AIMLSystems'22). Bangalore (Virtual Event), India.
7. June 2022. Theory and Practice of Multi-Party Computation Workshop (TPMPC). Aarhus, Denmark.
8. April 2022. The Network and Distributed System Security Symposium (NDSS). San Diego (Virtual Event), California.
9. August 2021. 8th Heidelberg Laureate Forum. Heidelberg (Virtual Event), Germany.
10. August 2021. The 30th USENIX Security Symposium (USENIX) 2021. (Virtual Event).
11. May 2021. EECS Research Students Symposium 2021. Indian Institute of Science (IISc), Bangalore (Virtual Event), India.
12. May 2021. Distributed and Private Machine Learning (DPML), ICLR Workshop 2021. (Virtual Event).
13. February 2021. 15th Academic Research and Careers for Students Symposium (ARCS) 2021. PSG College of Technology, Coimbatore (Virtual Event), India.
14. July 2020. EECS Research Students Symposium 2020. Indian Institute of Science (IISc), Bangalore (Virtual Event), India.
15. July 2020. International Symposium on Current Trends in Research and Innovation (ISCTRI'20). CHRIST University, Pune Lavasa Campus (Virtual Event), India.
16. February 2020. The 27th Network and Distributed System Security Symposium (NDSS) 2020. San Diego, USA.
17. February 2020. 14th Inter-Research-Institute Student Seminar in Computer Science (IRISS) 2020. Indian Institute of Technology (IIT) Gandhinagar, India.
18. January 2020. Secure Multi-Party Computation : Theory and Practice 2020. Indian Institute of Science (IISc), Bangalore, India.
19. November 2019. The 26th ACM Conference on Computer and Communications Security (CCS) 2019. London, United Kingdom.
20. December 2017. 18th International Conference on Cryptology (INDOCRYPT) 2017. The Institute of Mathematical Sciences (IMSc), Chennai, India.
21. March 2017. NMI Workshop on Secure Multiparty Computation. Indian Institute of Technology (IIT), Bomaby, India.
22. February 2017. The 24th Network and Distributed System Security Symposium (NDSS) 2017. San Diego, USA.
23. June 2016. Theory and Practice of Secure Multiparty Computation Workshop (TPMPC) 2016. Aarhus university, Denmark.
24. January 2016. 10th Inter-Research-Institute Student Seminar in Computer Science (IRISS) 2016. Trivandrum, India.